

N.Power

Hi-Power Wireless-N PoE AP usmjerivač

Korisnički priručnik







Autorska prava i odricanje od odgovornosti

OverLink Corp. je uložio velike napore u ispravnost informacija korisničkih uputama.

U slučaju pogreške ili neispravnosti podataka OverLink ne snosi odgovornosti.

Molimo koristite ga s oprezom. Sve informacije su promjenjive bez prethodnog upozorenja.

FCC izjava

Federal Communication Commission izjava o interferenciji. Uređaj je testiran i u skladu je s limitima klase B digitalnog uređaja, koji se odnosi na dio 15 FCC pravila.

Limiti su definirani radi pružanja zaštite protiv štetnih interferencija u naseljenim područjima. Oprema generira, koristi i može emitirati radio-frekvencijsku energiju te ako nije instalirana u skladu s uputama može uzrokovati štetne interferencije u radio komunikaciji. Međutim, ne postoji garancija da se interferencije neće pojaviti prilikom instalacije. U slučaju da uređaj uzrokuje štetne interferencije prema radio i televizijskom signalu, koja se može otkriti paljenjem i gašenjem opreme, korisnik može pokušati otkloniti interferenciju na jedan od sljedećih načina:

- Reorijentacija ili premještanje antene
- Povećati udaljenost između oprema i prijemnika
- Spojiti opremu na drugu utičnicu na strujni vod na kojom nije spojen prijemnik
- Kontaktirati dobavljača ili iskusnog radio/TV tehničara za pomoć

FCC pozor

Promjene i izmjene ove jedinice koje strana zadužena za sukladnost nije izričito odobrila mogu poništiti pravo korisnika na korištenje ove opreme.

Ovaj uređaj sukladan je dijelu 15 pravila Saveznog povjerenstva za komunikacije (FCC). Rad uređaja podložan je sljedećim dvama uvjetima:

- Uređaj ne smije uzrokovati štetne smetnje.
- Uređaj mora prihvatiti sve primljene smetnje, uključujući smetnje koje mogu uzrokovati neželjene radne karakteristike.

U SAD i Kanadi uređaj smije raditi samo na kanalima od 1 do 11. Ostale kanale nije moguće odabrati.
Uređaj i njegova antena/e ne smiju raditi s ostalim antenama ili odašiljačima.

VAŽNE NAPOMENE

FCC Izjava o izloženosti zračenju.

Ova oprema u skladu je s FCC ograničenjima izloženosti zračenju u nekontroliranom okruženju. Opremu je potrebno ugraditi i rabiti na udaljenosti od najmanje 20cm između odašiljatelja zračenja i osobe.





Sadržaj

1 Uvod

1.1 Pregled

N.Power je bežični multifunkcionalni usmjerivač baziran na 150 Mb/s bežičnoj b/g/n 2.4 GHz tehnologiji. Korisnici mogu dijeliti širokopojasnu internet vezu velike brzine. Sadrži četiri načina rada i na takav način zadovoljava različite okoline. Pored toga, omogućuje još pasivni PoE port za instalacije na mjestima koja u blizini nemaju pristup struji. Obratite pozornost na sljedeće značajke:

- N.Power podržava 12V na pasivnom PoE portu. Posebno ćete morati kupiti pasivni PoE ubrizgivač (PoE-1P). Za više informacija, pogledajte odjeljak 2.4.1.
- Maksimalna snaga slanja N.Power uređaja je oko 1 vat (30dBm). Međutim prema regulacijama sukladnosti limitiran je na 20 dBm u Europi i na 23 dBm u SAD-u. U usporedbi s klasičnim 11n usmjerivačima koji pružaju manje od 15 dBm izlazne snage, N.Power radi do 19 dBm (EU) i 22 dBm (FCC) u 11n načinu i time pruža veću pokrivenost. Unatoč mogućnostima N.Power preporučamo korištenje što je moguće manje snage zbog smetnji i štednje energije.
- N.Power dolazi s USB 2.0 portom za jednostavno dijeljenje putem FTP-a. Za podešavanje FTP-a, pogledajte Poglavlje 4.3.

U slučaju tehničkih problema, pročitate Poglavlje 10: Učestala pitanja.

1.2 Nadogradnja firmvera i tehnička podrška

Ako naiđete na tehničke probleme koje ne možete riješiti s ovim priručnikom, posjetite našu web stranicu www.airlive.com. Tehnička podrška s učestalim pitanjima se stalno ažurira.

U slučaju potrebe za nadogradnjom firmvera koji bi poboljšao funkcionalnost softvera ili popraviti nedostatak N.Power uređaja, možete pristupiti našem online centru za podršku na poveznici: http://www.airlive.com/support/support_2.jsp

2009 godine AirLive je dodao funkciju “Newsletter Instant Support System” koja omogućuje pretplatnicima primanje obavijesti kada se pojavi nova opcija za preuzimanje ili komentar na učestala pitanja za pretplaćene modele. Da bi postali AirLive pretplatnik posjetite stranicu http://www.airlive.com/member/member_3.jsp

Monthly news : ☑ Subscribe Language : English
Instant Support : ☑ Subscribe Language : English

☐ All Products

Product Main Category		Product Secondary Category		Model NO
Router		802.11a/b/g Products		
Security Gateway		802.11n Products		WN-301R
Skype		MIMO-G Products		WN-5000PCI
Switches		Turbo-G Products		WN-5000USB v2
VoIP	>>	802.11g+ Products	>>	WN-200R
Wireless Indoor		802.11g Products		WN-300USB
Wireless Accessory		802.11b Products		WN-360USB
Wireless Outdoor		GPR		WN-300R
WISP		WiFi Bundle Set		WN-200USB
Solutions				Traveler 3G

1.3 Funkcije

- Bežični-N AP usmjerivač
- Do 30dBm izlazne snage (20dBm u EU, 23 dBm u SAD)
- 1 x USB 2.0 Port
- 7 LED indikatora
- Hotspot autentifikacijska funkcija
- 150 Mb/s 1T1R bežični-b/g/n standard
- 12V pasivni POE Port
- WAN port za ADSL/kablovsku podršku
- Usmjerivački, AP, klijentski, premosni i repetitorski način
- Kontrola propusnosti
- 8MB Flash, 32MB SDRAM
- Zelena AP funkcija uštede energije
- Zidni držač i vijci
- Brzo obnavljanje firmvera

1.4 Radni načini

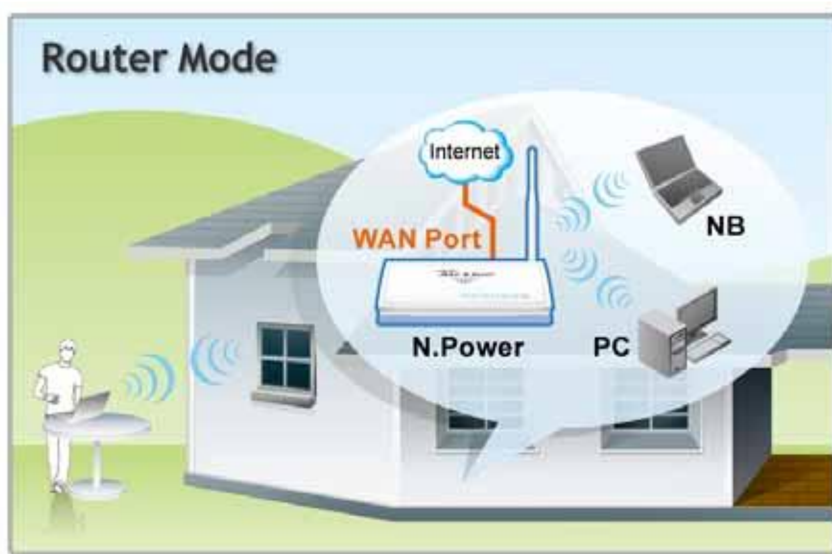
N.Power može raditi kao multi-funkcionalan bežični uređaj. Kroz AirLogic web sučelje, korisnik lako može odabrati radni način N.Power uređaja.

N.Power se može postaviti za rad u narednim načinima:

N.Power bežični način rada			
Bežični način	**Radio**	**WAN**	**Aplikacija**
Usmjerivač	AP	Da	Bežično dijeljenje Internet propusnosti
AP	AP	Nema	Samo Hotspot ili produžena udaljenost drugog WDS AP/usmjerivača
Klijent	Klijent	Nema	Spaja se na AP usmjerivač
WDS premosnik	WDS	Nema	Stvara vezu prema okosnici
WDS repetitor	AP + WDS	Nije dostupno	Pojačava bežični signal. Postavke WDS repetitora nalaze se unutar *Wireless Settings* postavki usmjerivačkog i AP načina rada.

1.4.1 Usmjerivački način rada

U ovom načinu možete dijeliti internet vezu žičano ili bežično. NAT funkcionalnost je dodijeljena za *IP sharing* funkciju od vašeg WAN porta prema LAN portovima i bežičnom sučelju.



1.4.2 AP način rada

Kada N.Power radi u *Access Point* načinu rada, onda se ponaša kao centralni koncentrator bežične mreže. Svi bežični uređaji i kartice komuniciraju kroz N.Power uređaj. Ova vrsta mreže poznata je pod nazivom *Infrastrukturna mreža* Ostali N.Power ili 802.11 b/g/n uređaji mogu se spojiti na AP putem klijentskog načina.



1.4.3 Klijentski način rada

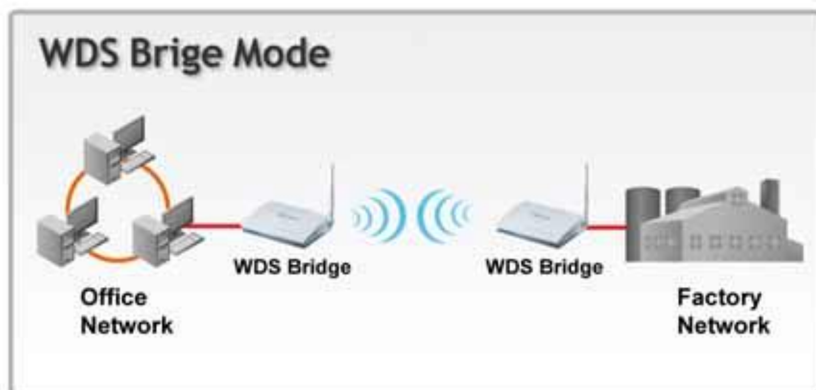
N.Power ponaša se kao bežični adapter koji se spaja s pristupnom točkom. Korisnici mogu spojiti računalo ili usmjerivač na LAN port N.Power za dobivanje mrežnog pristupa.



1.4.4 WDS prespojni način rada

Ovaj način koristi se za bežično povezivanje LAN mreža (na primjer između ureda i skladišta). WDS prespojnici koji koriste WPA-PSK ili WPA2-PSK enkripciju, mogu biti ograničeni samo na uređaje koje koriste isti bežični čipset.

WDS prespojnik radi na način da se unose MAC adrese udaljenog bežičnog prespojnika u WDS tablicu. MAC adresu možete pronaći na donjoj strani N.Power uređaja.

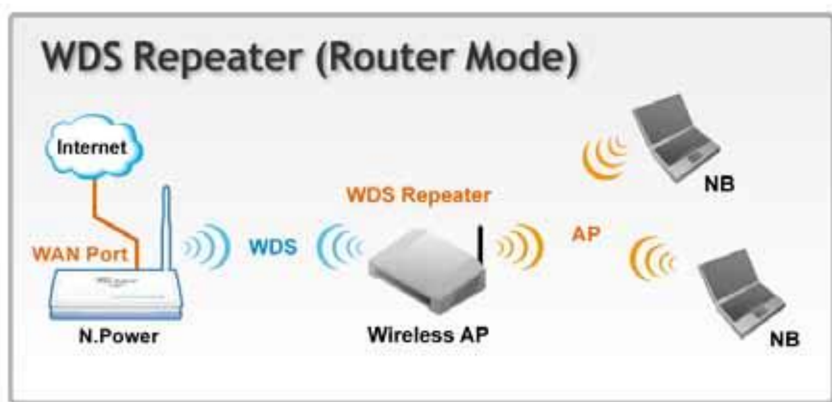


1.4.5 WDS repetitor način rada

Svrha repetitora je pojačavanje bežičnog signala udaljenog AP/usmjerivača. N.Power može raditi kao WDS repetitor unutar usmjerivačkog načina ili AP načina. WDS postavke možete pronaći na *Wireless Settings* stranici. Obje strane moraju podržati WDS vezu za rad.

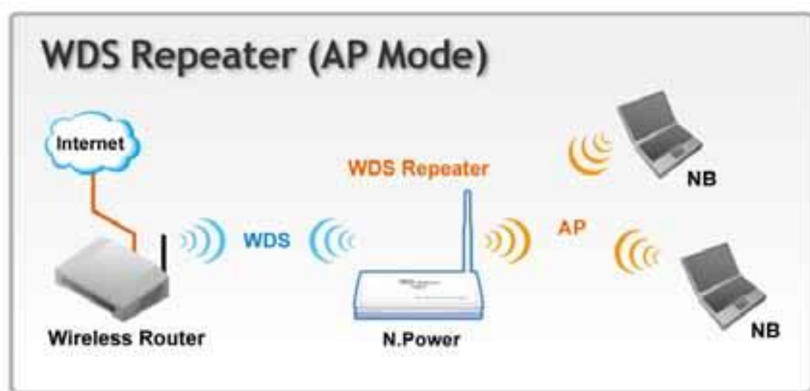
WDS repetitor u usmjerivačkom načinu

Uloga WDS repetitor funkcije u usmjerivačkom načinu rada je omogućavanje udaljenom AP pojačanje signala N.Power uređaja. Pogledajte sliku ispod.



WDS repetitor u AP načinu

Uloga WDS repetitor funkcije u AP načinu rada je pojačanje bežičnog signala udaljenog AP. Pogledajte sliku ispod.



Za informacije o podešavanju WDS repetitora, pogledajte odjeljak 4.4.10 i odjeljak 6.2.9.

2 Instaliranje N.Power uređaja

Ovaj odjeljak opisuje hardver i proceduru instalacije hardvera za N.Power. Za više detalja oko instalacije softvera, pogledajte Poglavlje 3.

2.1 Prije nego krenete

Važno je pročitati upute prije instalacije N.Power uređaja.

- LAN1 port radi kao pasivni PoE port.
- Antenu morate instalirati prije nego uključite uređaj u struju. U suprotnom, može doći do oštećenja. Oštećenje nastalo zbog nepoštivanja procedure instaliranja može poništiti jamstvo.
- Pasivni PoE DC ubrizgivač je opcionalan i nije uključen u paket. Molimo koristiti 12V pasivni PoE sustav s N.Power pasivnim PoE portom. Nemojte koristiti 802.3af 48V sustav ili PoE prespojnik s ovim uređajem.
- Radi smanjenja mogućnosti nastanka kvara na N.Power USB portu, isključite uređaj kada spajate ili odspajate USB uređaj iz USB porta.
- USB port podržava jednostavno dijeljenje putem FTP-a. Podržani su samo FAT ili FAT32 datotečni sustavi.
- FTP funkcija podržava samo datoteke sa zapadnom abecedom (poput engleske).
- Kada koristite USB tvrdi disk s N.Power uređajem, potreban je vanjski strujni adapter za USB tvrdi disk.

2.2 Sadržaj paketa

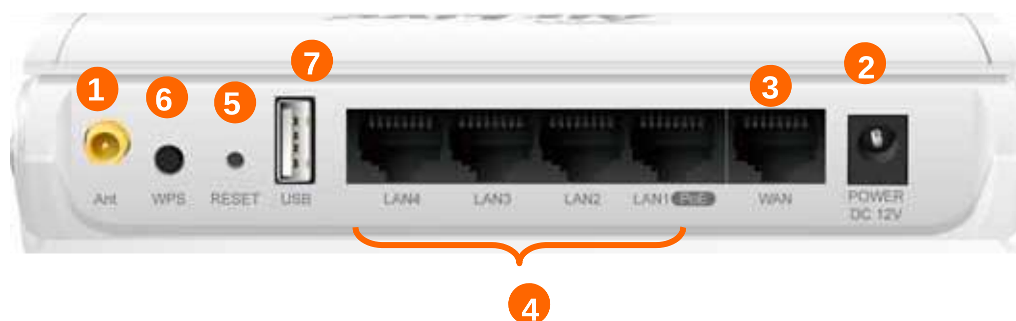
N.Power paket sadrži:

- Jedan N.Power uređaj
- Jedan 12V 1A DC strujni adapter
- Jedna antena
- CD S korisničkim uputama
- Vodič za brzi početak



2.3 Upoznavanje s N.Power uređajem

Ispod su prikazani opisi i slike uređaja.



1. Konektor za antenu
2. Konektor za strujni adapter
3. WAN Port
4. LAN Portovi (LAN1 za pasivni PoE Port)
5. Gumb za ponovno pokretanje
6. WPS gumb
7. USB Port (za USB pohranu)



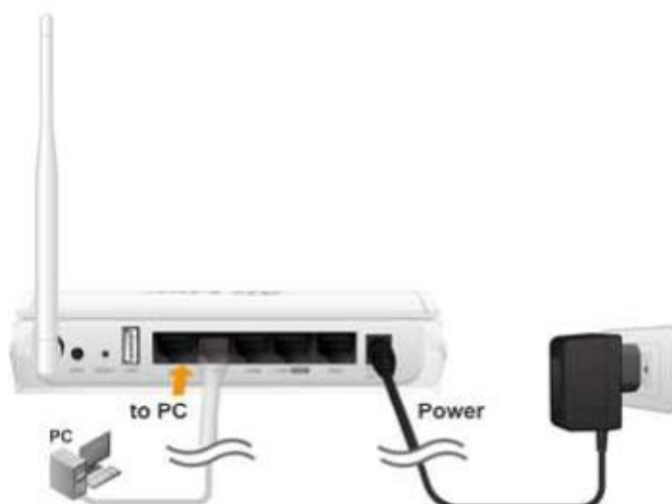
2.4 Instalacija hardvera

1. Instalirajte antenu na način da ju zavrnite u RF konektor u smjeru kazaljke na satu

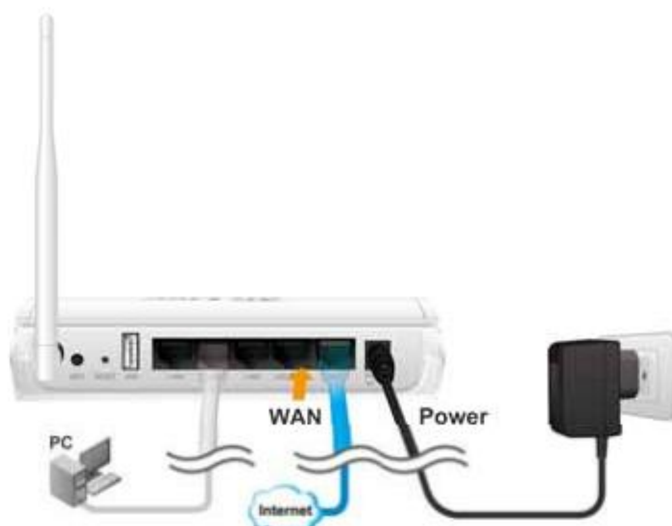
2. Spojite strujni adapter na N.Power.



3. Jedan kraj LAN kabla spojite na jedan od LAN portova, a drugi kraj spojite s računalom.



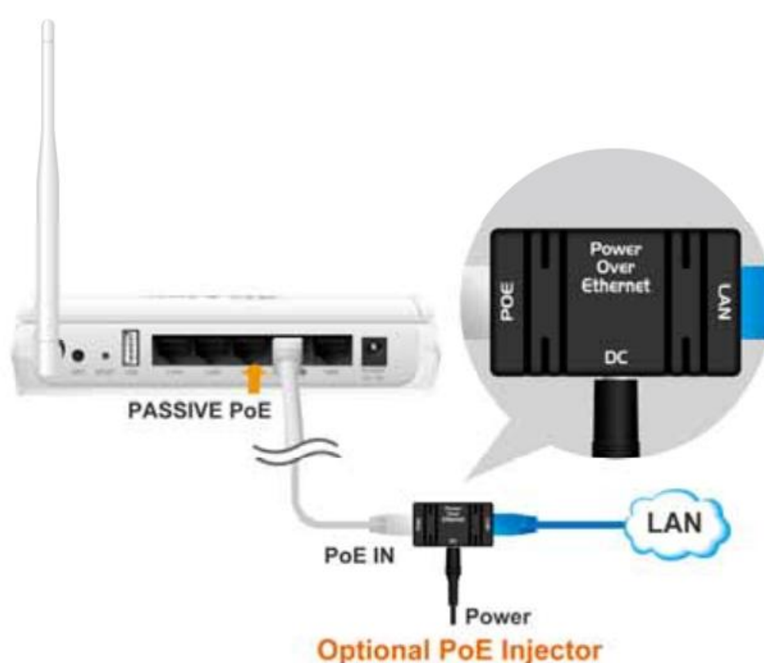
4. Ako imate širokopojasnu vezu, spojite kabel s WAN portom



5. Otvorite pretraživač i upišite 192.168.1.254 za pristup web upravljačkom sučelju.

2.4.1 Pasivna PoE instalacija

Ako imate napajanje preko pasivnog PoE, slijedite naredne upute za instalaciju. Pasivni DC ubrizgivač ne dolazi u paketu s N.Power te se mora kupiti odvojeno (AirLive Model: PoE-1P). N.Power koristi 12V pasivni PoE sustav te ne radi s 802.3af PoE prespojnikom ili 48V PoE opremom. Preporučuje se upotreba 12V DC i 12A ili više ako imate instaliran USB spremnik.



2.4.2 Instalacija držača na zid

1. Rupe za montiranje na zid nalaze se s donje strane uređaja. Izmjerite udaljenost između rupa i na istu tu udaljenost stavite vijke na zid. Nemojte ih skroz zavrnuti, nego ostavite malo mjesta za postavljanje N.Power uređaja.

2. Postavite N.Power na dva vijka.


2.5 LED tablica

U ovom odjeljku opisano je ponašanje LED lampica N.Power uređaja. LED lampice nalaze se s gornje strane N.Power uređaja.



WPS (Struja)
Postojano plava – Normali rad
Sporo treperenje: WPS pregled
OFF – Nema struje

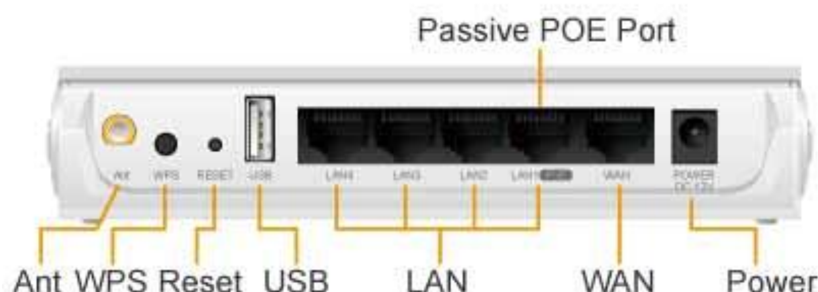
WLAN
Sporo treperenje: Signal je aktivan
Brzo treperenje: Prijenos podataka
OFF: Signal je onemogućen

LAN1 ~4 WAN

Postojano plava: Veza je uspostavljena
Brzo treperenje: Prijenos podataka
OFF: Nema veze

2.6 Vraćanje standardnih postavki

Ako ste zaboravili N.Power IP adresu ili zaporku, možete vratiti standardne postavke na način da pritisnete i držite „Reset" gumb duže od 10 sekundi. Za tu akciju možda će vam trebati olovka. „Reset" gumb nalazi se unutar okvira uređaja (pogledajte sliku ispod).



3 Podešavanje N.Power uređaja

N.Power nudi upravljačko sučelje putem web preglednika. U ovom poglavlju objasniti ćemo N.Power upravljačko sučelje.

3.1 Važne informacije

Naredne informacije pomoći će vam za brzi početak. Međutim, preporučljivo je pročitati kompletni priručnik prije početka. Obratite pozornost da su zaporka i SSID osjetljivi na velika i mala slova.

- Standardna IP adresa je: 192.168.1.254   Maska podmreže: 255.255.255.0
- Standardni korisnik je “admin”
- Standardna zaporka je “airlive”
- Standardni SSID je “airlive”
- Standardni bežični način je: Router mode (Usmjerivački način)
- Stisnite “Apply Change” za aktiviranje postavki.
- Nakon postavljanja postavki ponovno pokrenite uređaj “Reboot”.
- Brzo obnavljanje firmvera radi samo kada se spojite na LAN 1~4
- DHCP poslužitelj je standardno uključen u usmjerivačkom načinu rada. Kod drugih načina, DHCP poslužitelj je isključen. Kod prebacivanja s usmjerivačkog načina na ostale načine, morate ručno postaviti IP adresu računala.
- Regulacijsko tijelo za Europu je „ETSI“. Ako ne živite u europskoj državi možete promijeniti regulatornu domenu. Nemojte mijenjati regulacijsku domenu ako se ne odnosi na vašu zemlju jer korištenje pogrešne regulacijske domene može biti protuzakonito.
- Za upute oko postavljanja FTP funkcije pogledajte Poglavlje 4.3.

3.2 Priprema računala

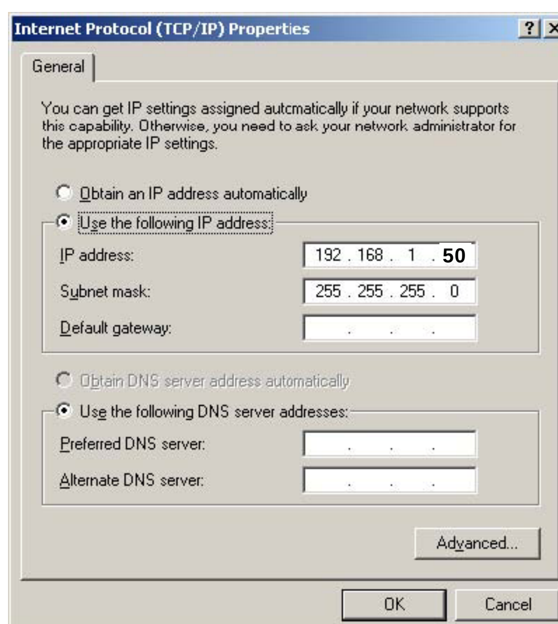
N.Power se može administrirati pomoću udaljenog računala koje je spojeno žičano ili bežično na mrežu. Standardna IP adresa N.Power uređaja je **192.168.1.254,** a maska podmreže je 255.255.255.0. To znači da IP adresa računala treba bit u rasponu od 192.168.1.1 do 192.168.1.253.

Za pripremu računala za upravljanje N.Power uređaja, slijedite naredne upute:

1. Spojite računalo s LAN portom N.Power uređaja

2. IP postavke postavite na *Obtain an IP address Automatically*. Ispravnu IP adresu trebali bi dobiti od N.Power uređaja.

3. Ako želite postaviti IP adresu ručno, postavite ju na 192.168.1.50 (ili na drugu adresu u istoj mreži).



Sada ste spremni za postavljanje N.Power uređaja pomoću računala.

3.3 Uvod u web upravljačko sučelje

N.Power upravljačkom sučelju može se pristupiti upisom IP adrese u web preglednik. Većina funkcija N.Power uređaja dostupna je kroz web sučelje.

Ako se N.Power uređaj nalazi iza usmjerivača ili vatrozida, možda ćete trebati otvoriti port 80 kao virtualni poslužitelj na vašem vatrozidu / usmjerivaču. Ova procedura nije potrebna u većini slučajeva ukoliko se između računala i N.Power uređaja ne nalazi usmjerivač / vatrozid.

3.3.1 Pristup web upravljačkom sučelju

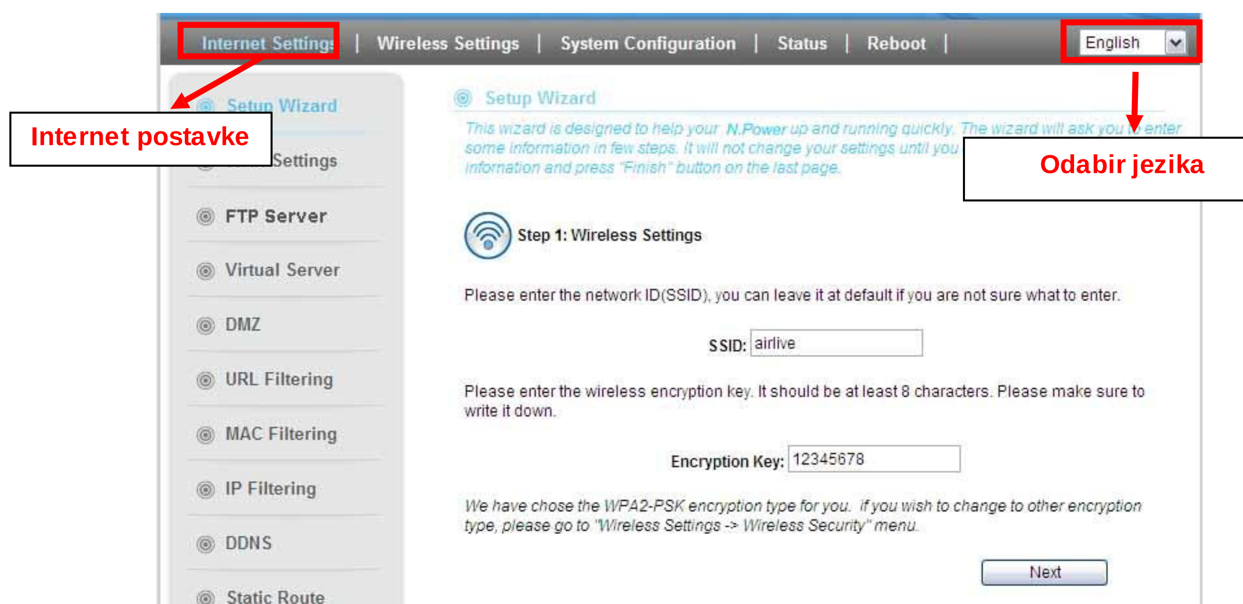
Za pristup normalnom upravljačkom sučelju, unesite N-Power IP adresu u web preglednik (standardna IP adresa je 192.168.1.254).



3.3.2 Struktura web sučelja

Preporučljivo je proći kroz sve opcije N.Power web upravljačkog sučelja za dobivanje šire slike o funkcijama i sučelju.

Nakon pristupa web upravljačkom sučelju, pojaviti će se naredni ekran:



- **Internet Settings:** Kada odaberete *Router mode*, pojaviti će se opcija *Internet Settings* u kojima ćete moći modificirati postavke. Izbornik neće biti dostupan kada odaberete drugi način rada.
- **Wireless Settings**: N.Power bežične postavke drukčije su za različite bežične načine. Radi pojednostavljenja sučelja prikazati će se samo funkcije koje su primjenjive za određeni način rada. Iz ovog izbornika možete promijeniti način rada. Za objašnjenje različitih načina rada pogledajte Poglavlje 1.
- **System Configuration:** Sve postavke nebežičnog i usmjerivačkog načina rada prikazane su u ovom dijelu: mijenjanje zaporke, dodavanje firmvera, kreiranje sigurnosne kopije i sl.
- **Status**: Služi za nadzor N.Power uređaja. Pruža informacije o uređaju, statističke podatke, klijentske zapise i sl.
- **Reboot:** Većina postavki za usvajane promjena zahtjeva ponovno pokretanje klikom na „Reboot“ gumb.
- **Language Selection:** Možete promijeniti jezik web sučelja.

3.4 Čarobnjak za konfiguraciju

Čarobnjak za konfiguraciju je prvi ekran koji će se prikazati kada se prijavite. Pitati će vas par pitanja oko postavljanja vaše bežične i širokopojasne veze.

Korak 1: Unesite svoj SSID i enkripcijski ključ. Standardni enkripcijski tip je WPA2-PSK (AES). Enkripcijski ključ trebao bi se sastojati od barem 8 alfanumeričkih znakova.

Setup Wizard

This wizard is designed to help your N.Power up and running quickly. The wizard will ask you to enter some information in few steps. It will not change your settings until you enter all the required information and press "Finish" button on the last page.

Step 1: Wireless Settings

Please enter the network ID(SSID), you can leave it at default if you are not sure what to enter.

SSID: airlive

Please enter the wireless encryption key. It should be at least 8 characters. Please make sure to write it down.

Encryption Key: 12345678

We have chose the WPA2-PSK encryption type for you. if you wish to change to other encryption type, please go to "Wireless Settings -> Wireless Security" menu.

Next

Korak 2: Odaberite vrstu širokopojasne veze. Ako niste sigurni oko odabira postavki, kontaktirajte svog ISP radi pružanja informacije.

Setup Wizard

WAN

Step 2: WAN Configuration

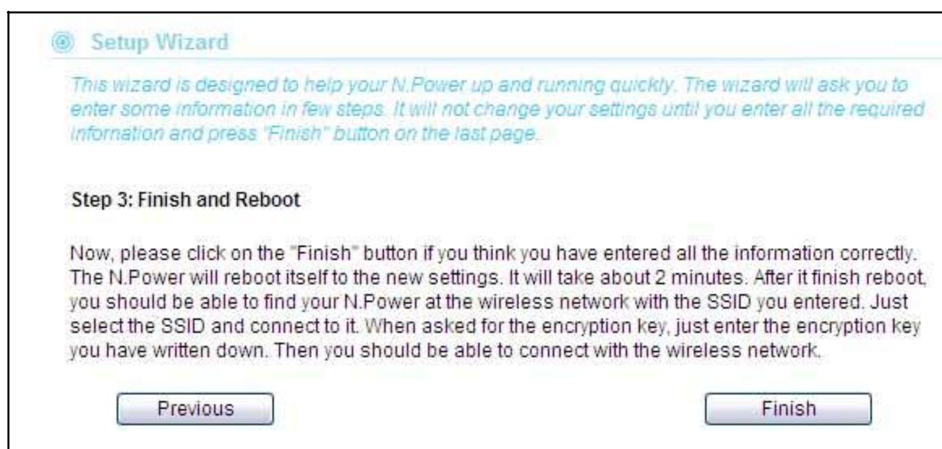
Please select and configure your Broadband Connection type. If you have ADSL service, your WAN type is likely to "PPPoE". If you have cable modem, your WAN type is likely to be "DHCP Client".

WAN Connection Type: DHCP Client

Static IP
DHCP Client
PPPoE
PPTP
L2TP
BigPond

Previous Next

Korak 3: Ako ste dobro postavili sve postavke kliknite na “Finish” za ponovno pokretanje sustava.



3.5 Mijenjanje radnog načina

Bežične postavke N.Power ovise o odabranom bežičnom radnom načinu. Za objašnjenje kako radi koji radni način, pogledajte Poglavlje 1.

Procedura promjene načina rada:

1. Odaberite *Wireless Setting*
2. Odaberite bežični način
3. AP vas može pitati za potvrdu promjene načina. Kada potvrdite, AP će se ponovno pokrenuti u novom načinu rada.

Napomena: *Kada promijenite iz usmjerivačkog načina rada u ostale načine, DHCP poslužitelj će biti isključen. U tom slučaju, morate ručno podesiti IP adresu računala da bude u istoj mreži kao i N.Power uređaj. Obrnuto, kada promijenite iz drugih načina rada u usmjerivački, DHCP poslužitelj će biti uključen.*

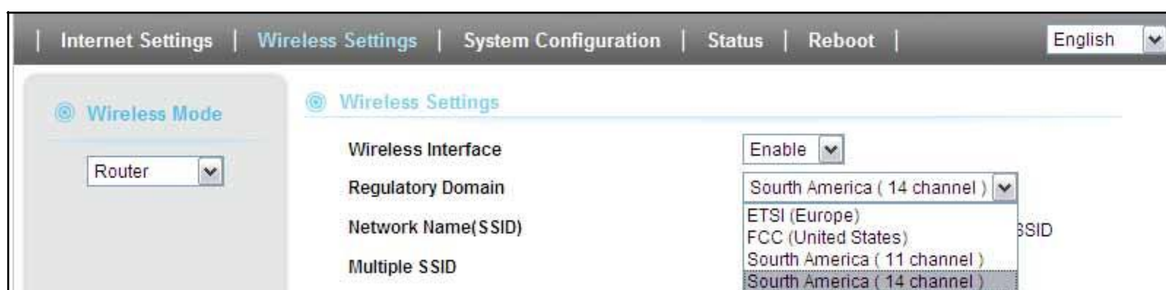


3.6 Promjena regulacijske domene

Postavljanjem regulacijske domene odrediti će se kanali i jačina izlazne snage koje će koristiti N.Power uređaj. Morate odabrati ispravnu regulacijsku domenu za vašu državu. Korištenje neispravne regulacijske domene može biti ilegalno (pogledajte tablicu ispod).
Ako niste sigurni koju regulacijsku domenu trebate koristiti, odaberite ETSI (Europe) i ograničite se na korištenje kanala od 1 do 11.

Tablica regulatorskih domena			
Domena	**Kanali**	**Maksimalna Tx izlazna snaga**	**Države**
ETSI (Europa)	1~13	20dBm	EU države
FCC (SAD)	1~11	23dBm	SAD i ostale države koje koriste WiFi regulative od SAD-a.
South America (11ch)	1~11	30dBm	Južno američke države koje koriste kanale FCC domene.
South America (14ch)	1~14	30dBm	Južno američke države koje dopuštaju korištenje svih kanala u 2.4GHz

Standardna regulacijsko tijelo je ETSI (Europe). Ako trebate promijeniti regulacijsku domenu, izbornik za promjenu domene nalazi se pod *Wireless Settings -> Regulatory Domain*. Nakon promjene regulacijske domene, uređaj će se ponovno pokrenuti s novim postavkama.



3.7 WPS (postavljanje WiFi zaštite)

WPS je sustav koji pojednostavljuje proces uspostave bežične sigurnosti. Postoje dva načina za podešavanje WPS veze:

1. **PBC** (Push Button Communication) hardverski / softverski:
   Stisnite WPS gumbe na AP-u i klijentskoj strani i WPS veza će se automatski uspostaviti. WPS gumb nalazi s donje strane N.Power uređaja.

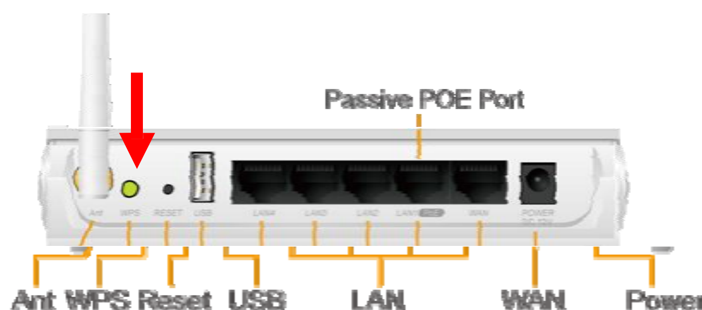
2. **PIN** (Personal Information Number) *Enrollee* i *Registrar*:
   U *WPS Registrar* dio trebate unijeti *PIN Code* od *Enrollee* dijela. Tada će se WPS veza uspostaviti automatski.

Preporučuje se upotreba prve opcije pošto je puno jednostavnije za podešavanje.

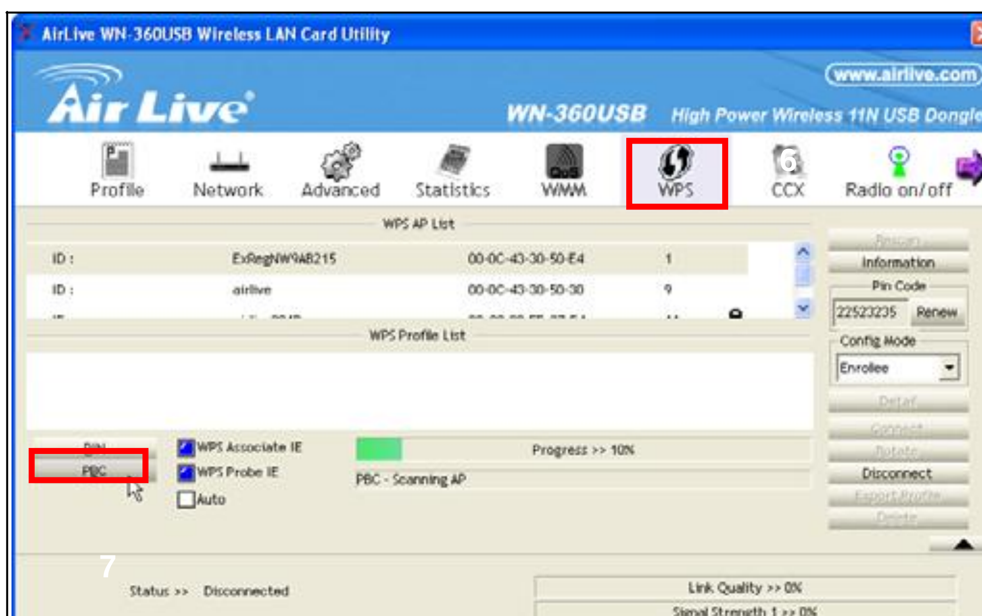
3.7.1 AP i usmjerivački načini

Primjer 1: Pomoću hardverskog gumba

Pritisnite WPS gumb na zadnjoj strani N.Power uređaja. WPS LED dioda će svijetliti i N.Power će započeti pretraživati WPS signale klijenata u trenutnoj okolini. U roku **dvije minute** morate uključiti bežičnu mrežnu karticu i kliknuti PBC za automatsko spajanje.

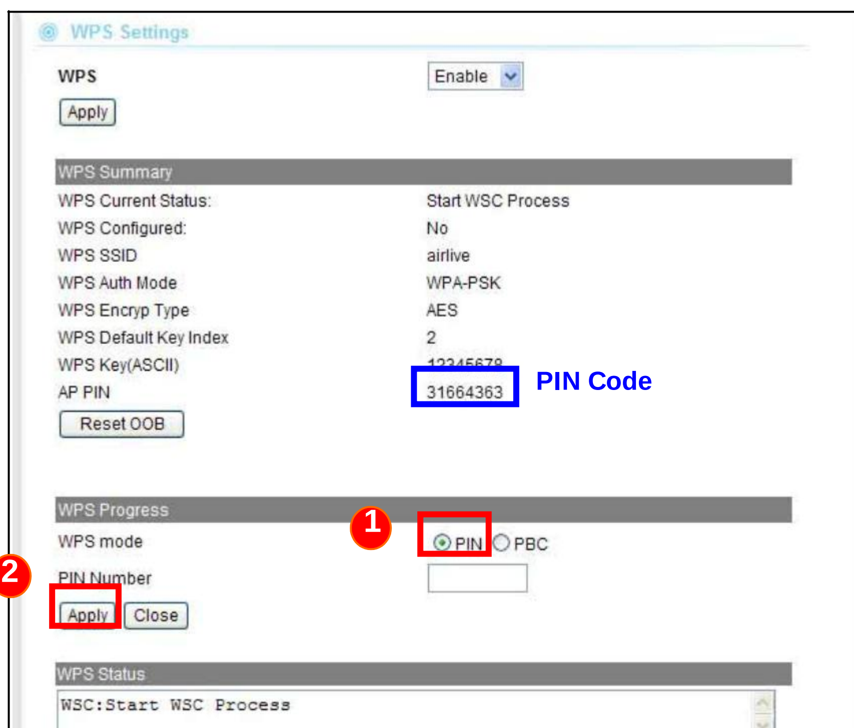


Ako imate hardverski WPS gumb na svojoj bežičnoj kartici, možete ga odmah stisnuti. Ako nemate, WPS PBC funkciju možete pronaći unutar bežičnog pomoćnog programa.
Ispod je prikazan primjer spajanja AirLive WN-360USB bežične mrežne kartice s N.Power uređajem.

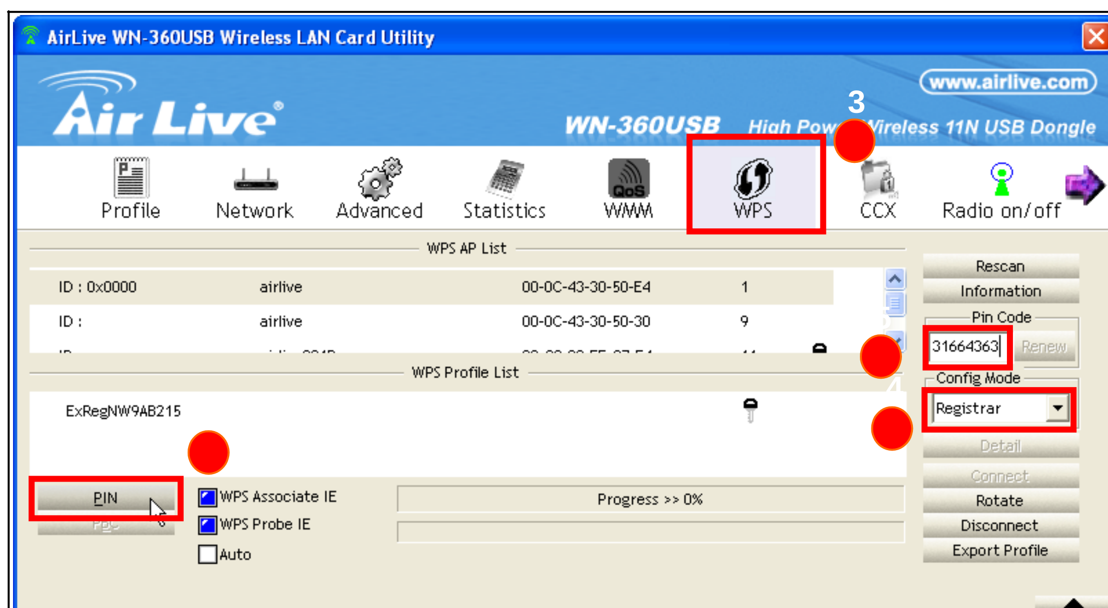


Primjer 2: WPS pomoću PIN-a

Prijavite se na N.Power kroz web korisničko sučelje. Odaberite *Wireless Setting -> WPS Setting.* U WPS dijelu odaberite „PIN“ i kliknite „Apply“. Dobiti ćete PIN kod.



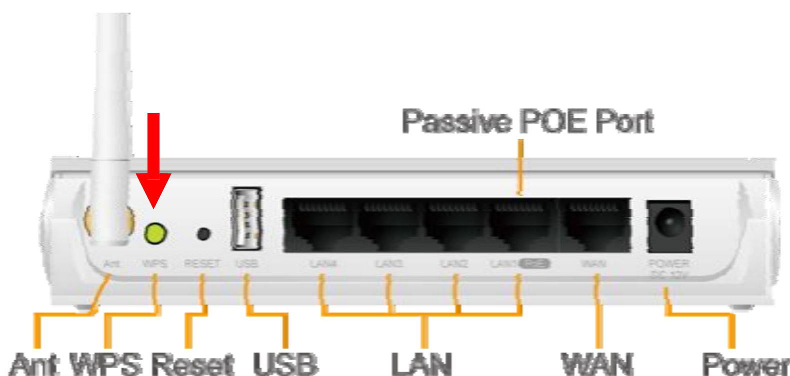
Uključite pomoćni program bežične mrežne kartice. Postavite WPS način na *Registrar* i unesite PIN kod. Pritisnite „PIN“ i veza će se automatski konfigurirati.



3.7.2 Klijentski način

Primjer 1: Pomoću WPS hardverskog gumba

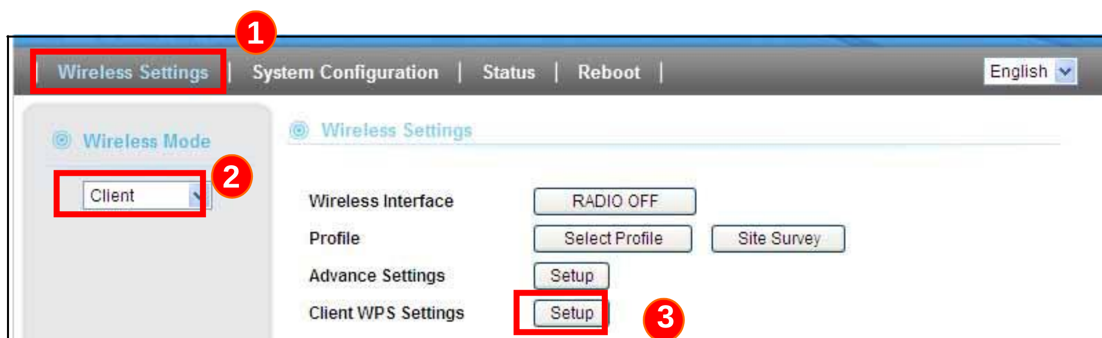
Pritisnite WPS gumb direktno na uređaju. WPS LED će zasvijetliti i N.Power će početi pretraživati AP WPS signal u okolini.



Unutar dvije minute, pritisnite WPS gumb na vašem AP uređaju i veza će se automatski uspostaviti.

Primjer 2: WPS pomoću PIN-a

Prijavite se na N.Power upravljačko sučelje. Odaberite *Wireless Setting -> Client mode -> Client WPS Setting.*



Odaberite SSID na koji se želite spojiti. Postavite WPS način na *Enrollee* za dobivanje PIN koda. Pritiskom na „PIN Start“ WPS LED dioda će dvije minute svijetliti na uređaju.

WPS Settings

WPS AP site survey								
No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
○	airlive300	00C002FFD070	55%	1	WPA2-PSK	AES	1.0	Conf.
○	Use3Gtest	000C43305030	100%	6	WPA2-PSK	AES	1.0	Conf.
○	airlive301R	00C002FFC7E4	100%	11	Unknown	WEP	1.0	Conf.
◉	airlive	000C433050EC	100%	1	OPEN	Not Use	1.0	Conf.

UUID:28802880288018800a880000c433050ec
RF Band:2.4G/5G

4 5 6 7

Refresh Mode: Enrollee PIN 85958968 **Copy PIN Code**

PIN Start PBC Start Cancel

Renew PIN

Close

Pod AP stranicom odaberite *Wireless Setting* -> *WPS Setting*. Postavite WPS način na „PIN“, unesite PIN kod i kliknite na „Apply“ za automatski uspostavljanje veze.

WPS Progress

8 9 10

WPS mode ◉ PIN ○ PBC

PIN Number 85958968 **Enter PIN Code**

Apply Close

4 Usmjerivački način

U ovom poglavlju biti će opisane bežične postavke u usmjerivačkom načinu rada.

4.1 Usmjerivački način

Usmjerivački način je glavni radni način N.Power uređaja. U ovom načinu možete dijeliti internet vezu žičano ili bežično. NAT funkcija primjenjuje se na IP dijeljenje od WAN port sučelja prema LAN portovima bežičnog mrežnog sučelja.



4.2 Izbornik internet postavki

Izbornik internet postavki je prvi prozor koji ćete vidjeti nakon prijave na N.Power uređaj. Sve opcije za WAN postavke mogu se pronaći ovdje. Ovaj izbornik neće se pojaviti u ostalim načinima rada.

4.2.1 Čarobnjak za postavke

Čarobnjak za postavke je prvi ekran koji će se pojaviti nakon što se prijavite. Pitati će vas nekoliko pitanja za brzo postavljanje bežičnih i širokopojasnih postavki.

Korak 1: Unesite svoj SSID i enkripcijski ključ. Standardni enkripcijski tip je WPA2-PSK (AES). Enkripcijski ključ trebao bi se sastojati od barem 8 alfanumeričkih znakova.

Setup Wizard

This wizard is designed to help your N.Power up and running quickly. The wizard will ask you to enter some information in few steps. It will not change your settings until you enter all the required information and press "Finish" button on the last page.

Step 1: Wireless Settings

Please enter the network ID(SSID), you can leave it at default if you are not sure what to enter.

SSID: airlive

Please enter the wireless encryption key. It should be at least 8 characters. Please make sure to write it down.

Encryption Key: 12345678

We have chose the WPA2-PSK encryption type for you. if you wish to change to other encryption type, please go to "Wireless Settings -> Wireless Security" menu.

Next

Korak 2: Odaberite vrstu širokopojasne veze. Ako niste sigurni oko odabira postavki, kontaktirajte svog ISP radi pružanja informacije.

Setup Wizard

WAN

Step 2: WAN Configuration

Please select and configure your Broadband Connection type. If you have ADSL service, your WAN type is likely to "PPPoE". If you have cable modem, your WAN type is likely to be "DHCP Client".

WAN Connection Type: DHCP Client

Static IP
DHCP Client
PPPoE
PPTP
L2TP
BigPond

Previous Next

Korak 3: Ako ste dobro postavili sve postavke kliknite na “Finish” za ponovno pokretanje sustava.

Setup Wizard

This wizard is designed to help your N.Power up and running quickly. The wizard will ask you to enter some information in few steps. It will not change your settings until you enter all the required information and press "Finish" button on the last page.

Step 3: Finish and Reboot

Now, please click on the "Finish" button if you think you have entered all the information correctly. The N.Power will reboot itself to the new settings. It will take about 2 minutes. After it finish reboot, you should be able to find your N.Power at the wireless network with the SSID you entered. Just select the SSID and connect to it. When asked for the encryption key, just enter the encryption key you have written down. Then you should be able to connect with the wireless network.

Previous   Finish

4.2.2 WAN postavke

Internet Settings -> WAN Settings

WAN Settings

WAN Connection Type: DHCP (Auto Config)
TTL: Disable
TTL Value: 32 (1-255)
MAC Address Clone: Disable

Enable UPnP
Enable Response to PING
Enable Remote Management

Enable IPSec Passthrough
Enable PPTP Passthrough
Enable L2TP Passthrough

Apply Change   Reset

- **WAN Connection Type:** Odaberite ISP vrstu veze. Ako koristite ADSL vezu, najvjerojatnija vrsta veze je PPPoE. Ako koristite kablovski modem, najvjerojatnija vrsta veze je DHCP. Međutim, bilo bi dobro kontaktirati vašeg ISP oko ispravnih postavki.
- **TTL:** Time to Live je 8-bitna vrijednost u IP zaglavlju. Vaš ISP može zahtijevati postavljanje ove postavke za ispravan rad. Kontaktirajte svog ISP i provjerite da li je TTL potreban, iako u većini slučajeva nije. Ako je potrebno postavljanje TTL, omogućite TTL i unesite vrijednost u polje ispod.

- **MAC address clone:** Ako je vaš ISP veže pristup Internetu na MAC adresu vašeg računala, možda ćete trebati omogućiti funkciju i unijeti MAC adresu računala.
- **Enable UPnP:** Omogućite univerzalni *plug and play.*
- **Enable Response to PING:** Omogućite ovo opciju ukoliko želite da N.Power odgovara na PING naredbu.
- **Enable Remote Management:** Omogućite ovu opciju za pristup web upravljačkom sučelju s udaljene lokacije.
- **Enable VPN Pass Through:** Ako imate postavljeni VPN poslužitelj u lokalnoj mreži morate omogućiti VPN prolaz i dopustiti udaljeni pristup VPN mrežama.

4.2.3 Virtualni poslužitelj

Internet Settings -> Virtual Server

Virtualni poslužitelj omogućuje definiranje jedne ili više aplikacija na poslužiteljima u LAN-u kojima mogu pristupiti svi internet korisnici. Internet podaci namijenjeni za određeni javni port biti će usmjereni na specifični privatni port LAN klijenta sa specifičnom privatnom IP adresom.

Ukoliko želite omogućiti pristup do vašeg web poslužitelja, FTP poslužitelja ili mail poslužitelju, morati ćete otvoriti specifični port na virtualnom poslužitelju prema lokalnoj IP adresi.

N.Power uređaj nudi *Copy PC* i *Pre-defined* servis za pojednostavljenje procesa kreiranje virtualnog poslužitelja.

Primjer 1: Otvaranje FTP servisa prema računalu

Korak 1: Omogućite funkciju virtualnog poslužitelja

Korak 2: Kliknite na “Copy PC” ikonu za kopiranje IP adrese vašeg računala.

Korak 3: Kliknite na “Pre-Define” za dobivanje liste popularnih servisa i kliknite “FTP”.

Korak 4: Kliknite na “Apply” i novi virtualni poslužitelj trebao bi se pojaviti u tablici.

Virtual Server

This function will open up specific ports for internet server or application to your PC. For example, you need to port 80 TCP/UDP for web server function. If you are not sure what port to open, please press the "Pre-Defined" button to select the most frequent used Virtual Servers.

Virtual Server Settings: Enable
IP Address: 192.168.1.25 COPY PC
Port Range: 20 - 21 Pre-Defined
Protocol: TCP
Comment:
(The maximum rule count is 32)

Apply Reset

Current Virtual Servers in system

No.	IP Address	Port Range	Protocol	Comment
1 ☐	192.168.1.25	20 - 21	TCP	FTP service

Delete Selected Reset

Za popis najčešće upotrebljavanih TCP i UDP portova posjetite poveznicu ispod:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

4.2.4 DMZ

Internet Settings -> DMZ

DMZ otvara sve TCP/UDP portove prema određenoj IP adresi s LAN strane. Uglavnom se koristi kod postavljanje poslužitelja za igre iza N.Power uređaja.

4.2.5 URL filtriranje

Internet Settings -> URL Filtering

N.Power pruža funkciju URL filtriranja za sprečavanje pristupa određenim web stranicama. Npr: roditelji na takav način mogu djeci zabraniti pristup određenim stranicama.

URL Filtering

URL filtering can restrict access to certain websites.

URL Filtering Disable

Apply Change

Add URL Address:

Add Reset

Current Webs URL Filters

URL	Number

Delete Selected Delete All Reset

4.2.6 MAC filtriranje

Internet Settings -> MAC Filtering

MAC filter može filtrirati promet od određene MAC adrese. Može spriječiti pristup internetu s određene stanice u lokalnoj mreži. Unesite MAC adresu u XX-XX-XX-XX-XX formatu. Na primjer: 00-4F-66-11-22-33.

MAC Filtering

MAC Filtering can block all traffic from certain MAC addresses.

MAC Filtering Disable

Apply Change

MAC Address

Add Reset

MAC Filtering Table

MAC Address	Number

Delete Selected Delete All Reset

4.2.7 IP filtriranje

Internet Settings -> IP Filtering

IP filtriranje omogućuje blokiranje pristupu mreži s određene IP adrese.

IP Filtering

IP Filtering can block all traffic from certain IP address. This might be useful to stop virus or hacker a

IP Filtering Disable

Apply Change

Destination IP Address

Source IP Address

Apply Reset

IP Filtering Table		
Dest IP Address	Source IP Address	Number

Delete Selected Delete All Reset

4.2.8 DDNS

Internet Settings -> DDNS

Dynamic Domain Name System. Algoritam koji dopušta upotrebu dinamičke IP adrese za postavljanje internet poslužitelja. DDNS servis omogućuje svakom korisniku račun s domenskim imenom. N.Power podržava "Dyndns.org", "zoneedit.com" i "no-ip.com" servis.

DDNS Settings

Dynamic DNS allow relating a domain to your router's WAN IP address, even if the address is not static.

Dynamic DNS Disable

Apply Change

Dynamic DNS Provider None

Account

Password

DDNS

Result

Apply Cancel

4.2.9 Statičke rute

Internet Settings -> Static Route

Statičke rute omogućuju ručno definiranje usmjerivačkih tablica.

Static Route

Add a routing rule:

Destination
Range Host
Gateway
Interface LAN
Comment

Apply Reset

Routing Table

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
3	192.168.7.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
4	239.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	LAN(br0)	

Delete Selected

4.3 FTP funkcija

N.Power USB port podržava dijeljenje podataka uz pomoć FTP funkcije. Možete spojiti USB spremnik na USB port za brzo dijeljenje podataka s prijateljima i obitelji. Prije nego krenete, proučite zahtjeva i ograničenja FTP funkcije:

- FTP funkcija dostupna je samo u usmjerivačkom načinu rada.
- USB spremnik podržava samo FAT ili FAT32 datotečne sustave.
- FTP funkcija podržava samo imena zapadnih abeceda (poput engleske)
- Kada koristite USB tvrdi disk s N.Power uređajem, potrebno je vanjsko napajanje za USB tvrdi disk.
- Nemojte spajati ili odspajati USB spremnik dok je usmjerivač uključen. Isključite napajanje prije spajanje ili odspajanja USB spremnika.
- N.Power podržava anonimne ili šifrirane FTP račune. Podržava do 3 šifrirana računa.

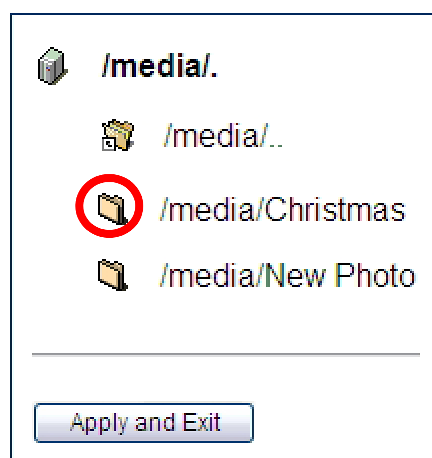
FTP možete konfigurirati u dijelu *Internet Settings*. Standardno je onemogućena te ju morate uključiti za početak korištenja. Kada napravite izmjene kliknite na „Apply“ prihvaćanje promjena.

- **Enable FTP Server:** Standardno FTP poslužitelj je onemogućen. Omogućite funkciju klikom na „Enable FTP Server“ i kliknite na „Apply“.
- **Service Port:** Možete promijeniti pristupni FTP port. Standardni port je 21; preporučuje se ostaviti standardne vrijednosti. Kada promijenite FTP port, FTP poveznica će se također promijeniti. Na primjer: ako promijenite broj porta na 2121, LAN FTP poveznica postati će ftp://192.168.1.254:2121.
- **Internet Link:** N.Power će automatski prikazati FTP poveznicu tako da ćete ju moći lako kopirati i poslati prijateljima. FTP poveznica dostupna je putem interneta.
- **Local LAN Link:** Lokalna poveznica unutar LAN preko koje možete pristupiti FTP datotekama. Za pristup pritisnite gumb „Copy Link“ i zalijepite ga u vaš preglednik.
- **Account Type:** Postoje dva različita tipa FTP računa:
  - **Anonymous (No Password):** Ne postoji zaštita za račun. Svi imaju pristup do FTP mape. Pristup je *Read only*, što znači da možete preuzeti podatke, ali ih ne možete postaviti.
  - **Password**: Može se definirati maksimalno 3 računa i svaki zahtjeva korisničko ime i zaporku. Svaki korisnik može imati različitu mapu za dijeljenje. Možete odabrati „Read“ i/ili „Write“ način pristupa za svaki tip računa. Kada odaberete tip računa „Password“ pojaviti će se sljedeći prozor:

Account Type: Password Access

Account	Username	Password	Read	Write	Directory
1			☐	☐	Browse
2			☐	☐	Browse
3			☐	☐	Browse

Username: Ime korisničkog računa.
Password: Potrebna zaporka za FTP pristup.
Read: Pravo za čitanje/preuzimanje s N.Power uređaja. Treba biti omogućeno.
Write: Pravo pisanja/postavljanja datoteka na N.Power uređaj.
Directory: Određivanje dijeljene mape za N.Power uređaj. Možete ručno unijeti putanju (počinje s "**/media/**") ili kliknuti na gumb "Browse" za odabir mape. N.Power može čitati do 5 razina mapa.
Browse: Odabir mape za dijeljenje. Za navigaciju mapama kliknite na "Directory Icon" . Kada završite kliknite na „Apply and Exit".



4.4 Izbornik bežičnih postavki

Kada u gornjem izborniku odaberete "*Wireless Settings*", pojaviti će se naredni prozor:

4.4.1 Regulacijska tijela

Wireless Settings -> Regulatory Domain

Regulacijske domene određuju koji kanali i koja razina Tx izlazne snage je dostupna u vašoj zemlji. U većini slučajeva regulacijska domena je ispravno odabrana. Budite svjesni da je korištenje neispravne regulacijske domene strogo zabranjeno. Ako živite u Europe morate koristiti ETSI regulatorsku domenu. Ako živite u SAD-u morate koristiti FCC domenu.

N.Power je usklađen s narednim regulacijskim tijelima:

Regulacijsko tijelo	Dostupni kanali	Maksimalna Tx izlazna snaga
ETSI (Europa)	1 ~13	20dBm
FCC (SAD)	1~11	23dBm
Južna Amerika (11 CH)	1~11	30dBm
Južna Amerika (14 CH)	1~14	30dBm

4.4.2 Višestruki SSID

Wireless Settings -> Multiple SSID

Višestruki SSID dopušta kreiranje maksimalno 4 različite bežične mreže (SSID). Funkcija je poznata pod nazivom „Virtual AP“. Svaki SSID može imati svoju politiku šifriranja. SSID1 je glavna bežična mreža unutar *Wireless Settings* stranice.

- **Hide SSID**: Bežična mreža postati će nevidljiva te će biti dostupna samo osobama koji znaju naziv SSID-a.
- **Enable Isolation between SSIDs**: Uključivanje opcije onemogućiti će promet između različitih bežičnih mreža.

4.4.3 Kanali

Wireless Settings -> Channel

Kanal predstavlja frekvencijski rang za prijenos signala. U 802.11 g/b standardu postoji maksimalno 14 kanala. Međutim, dostupnost kanala u svakoj zemlji ovisi o lokalnim regulacijama. Ako živite u Europi, možete koristiti kanale od 1 do 13, a ako živite u SAD-u, onda možete koristiti kanale od 1 do 11.

Svaki bežični kanal nalazi se u frekvencijskom rangu od 22 do 25 MHz, ali su kanali odvojeni samo 5MHz. Zbog toga, samo je svaki 5 kanala slobodan od interferencija s drugim kanalima. Preporučljivo je istražiti i saznati koje kanale koriste okolne pristupne točke te odabrati slobodni kanal.

4.4.4 Bežična zaštita

Wireless Settings -> Wireless Security

Preporučljivo je odmah postaviti bežičnu zaštitu i osigurati siguran prijenos podataka i spriječiti neovlašteni pristup. **Najlakši način postavljanje zaštite je pomoću čarobnjaka *Setup Wizard*. Čarobnjak automatski odabire najsigurniju i najlakšu shemu za zaštitu vaše bežične mreže.** Ukoliko želite sami postaviti sigurnosnu zaštitu, N. Power nudi različite enkripcijske modele poput: WEP, WPA-PSK, WPA, WPA2, WPA2-PSK. Općenito, WPA-PSK i WPA2-PSK su najpopularnije i najsigurnije metode zaštite.

Procedura postavljanja zaštite



- **Korak 1**: **Select your SSID:** Ako ste omogućili „Multiple SSID“ u padajućem izborniku pojaviti će mogućnost odabira različitog SSID-a. Svaki SSID (Virtualni AP) može imati vlastitu politiku zaštite.
- **Korak 2**: **Odabir „Security Policy“**: N.Power nudi široki raspon sigurnosnih politika uključujući: WEP (Pre-Shared Key), WPA (certificate), WPA-PSK (AES), WPA2-PSK (AES) i 802.1x *Radius Authentication*. Nedavno su WiFi regulacije zabranile korištenje TKIP enkripcije u 11n standardu, te je TKIP dostupan samo u 11 b/g standardu. Preporučuje se upotreba WPA-PSK AES sigurnosnog protokola kao najjednostavnijeg i najsigurnijeg načina zaštite.

4.4.5 Kontrola pristupa

Wireless Settings -> Access Control

N.Power omogućuje definiranje liste MAC adresa koje imaju mogućnost pristupa mreži ili kojima je zabranjen pristup bežičnoj mreži. Funkcija je dostupna samo u AP i AP usmjerivačkom načinu rada.



- **Disable:** Onemogućuje MAC filtriranje.
- **Allow list:** Kada se odabere, podatkovni promet u mreži biti će dopušten samo uređaja koji su navedeni u tablici.
- **Deny list:** Kada se odabere, podatkovni promet u mreži biti će zabranjen samo uređaja koji su navedeni u tablici.

4.4.6 Kontrola propusnosti

Wireless Settings -> Bandwidth Control

N.Power može limitirati propusnost po IP ili MAC adresi. Prvo omogućite opciju *Bandwidth Control* i tada odaberite „IP Control“ ili „MAC Control“.

- **Enable Bandwidth Control:** Za omogućavanje kontrole propusnosti, označite polje i kliknite na “Apply Change”.
  - **IP Control:** Limitiranje propusnosti jedne IP adrese.
  - **MAC Control:** Limitiranje propusnosti jedne MAC adrese.
  - **Upload Bandwidth:** Unesite limit postavljanja u Kb/s.
  - **Download Bandwidth:** Unesite limit preuzimanja u Kb/s.
  - **Comment:** Napomena za politiku dodjele propusnosti.

QoS

You may configure QoS Bandwidth Management here.

Enable QoS

Apply Change

IP Control

IP Address

Upload Bandwidth Kbps

Download Bandwidth Kbps

Comment

Apply Reset

Bandwidth Policy Table

IP Address	MAC Address	Download	Upload	Comment	Select

Delete Selected Delete All Reset

4.4.7 Dodijeljeni klijenti

Wireless Settings -> Associated Client

Status bežičnih klijenata možete provjeriti u tablici ispod.

Client Tables

You could monitor stations which associated to this AP here.

Associated Clients

MAC Address	Power Saving	Modulation	Channel Width	RSSI(dB)	Time(Sec)
00-0C-43-30-50-80	0	7	40M	-61	58

Close

- **MAC Address**: MAC adresa bežičnih klijenata. Ako želite pronaći IP adresu, pogledajte pod **Status -> Client Table**.
- **Power Saving**: **0**: Ušteda energije je isključena. **1**: Ušteda energije je uključena.
- **Modulation**: Prikazuje koji MCS nivo se koristi u 11n načinu.
- **Channel Width**: Definira da li klijent koristi 20 MHz ili 40 MHz širinu kanala.
- **RSSI (dBm)**: Snaga signala klijentskog uređaja.
- **Time (Sec)**: Koliko je dugo vremena je spojen bežični klijent.

4.4.8 Napredne postavke

Wireless Settings -> Advance Settings

- **Channel Width:** Možete odabrati širinu kanala od 20 MHz ili 20/40 Mhz. Odaberite 20 MHz zbog sukladnosti sa zakonom u nekim državama. 40MHz nudi bolje performanse od 20 MHz.

- **Guard Interval**: *Guard Interval* nalazi se na početku svakog prijenosa. Koristi se za smanjenje efekta miješanja višestrukih putanja prijenosa. Korištenje dugog *Guard Intervala* može smanjiti miješanje u višestrukom okruženjima, ali zato može smanjiti performanse.

- **MCS (Modulation and Code Scheme):** MCS nivo za 11n standard. Preporuča se ostaviti postavku na Auto.

Advance Setup

Channel BandWidth	20 / 20/40 (selected)
Guard Interval	long / Auto (selected)
MCS	Auto
Decline BA Request	Disable (selected) / Enable
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	Enable / Disable (selected)
Short Slot	Enable (selected) / Disable
Tx Burst	Enable (selected) / Disable
Pkt Aggregate	Enable (selected) / Disable
TX ACK Timeout	32 usec
RX ACK Timeout	10 usec
Calculate ACK Timeout value	Calculate
Multicast-to-Unicast	Enable / Disable (selected)

Apply Change   Close

- **Decline BA Request:** Omogućite opciju za odbijanje *Block ACK* zahtjeva od drugih uređaja

- **BG Protection:** 802.11g standard uključuje mehanizam zaštite koji pruža zajednički rad 802.11b i 802.11g standarda. Ukoliko nema takovog mehanizma, dvije vrste standarda mogu se međusobno miješati i smanjiti mrežne performanse.

- **Beacon Interval:** Uređaj redovito emitira ispitne poruke da bi obznanio svoju postojanost. Ispitna poruka (Bacon Interval) definira koliko često se ispitna poruka prenosi u jedinici vremena u milisekundama. Standardna vrijednost je 100, a ispravna vrijednost trebala biti između 1 i 65.535.

- **Fragmentation:** Kada veličina *unicast* poruke prelazi fragmentacijski prag, onda će biti fragmentirana prije prijenosa. Trebala bi imati vrijednost od 356 do 2346 bajtova, sa standardnom vrijednosti 2346. Ukoliko dođe do visokog nivoa pogrešno prenesenih paketa, trebali bi smanjiti fragmentacijski prag.

- **RTS Threshold:** RTS/CTS okviri koriste se za kontrolu medija za prijenos. Sve *unicast* poruke (podaci ili kontrola) veće od definiranog RTS praga, mogu se prenijeti nakon RTS/CTS mehanizma razmijene.

RTS prag bi trebao imati vrijednost između 256-2347 bajtova, dok je standardna vrijednosti **2347**. Nije preporučljivo preveliko odstupanje od standardne veličine.

- **Short Preamble**: Preambula je signal koji se koristi u bežičnom okruženju za sinkroniziranje vremena prijenosa pomoću *Synchronization* i *Start* okvirnog graničnika. U „bučnim" mrežnim okolinama, tip preambule trebao bi biti postavljen na dugu preambulu (Long Preambule). Kratka preambula (Short Preambule) koristi se kod aplikacija koje su minimalno zahtjevne i koje traže maksimalne performanse. U „bučnom" mrežnom okruženju, performanse će se smanjiti.

- **Tx Burst and Packet Aggregate:** Postoje sheme za poboljšanje performansi prijenosa podataka u 11n i Turbo standardima. Preporučljivo je omogućiti ove opcije.

- **AckTimeOut:** Kada bežična stanica pošalje paket prema drugoj bežičnoj stanici, čekati će na potvrdi okvir (Acknowledgement Frame) od nje. Stanica će čekati samo određeno vrijeme, a to vrijeme se zove *ACK timeout*. **Standardne vrijednosti *Tx i Rx timeout-a* su točne u većini slučajeva te ih nije potrebno mijenjati.**

4.4.9 WMM postavke

Wireless Settings -> WMM Settings

Wi-Fi Multimedia (WMM) je standard za prioritiziranje multimedijalnih aplikacija. WMM postavke služe za podešavanje višestrukih redova čekanja za postizanje boljih performansi različitih bežičnih paketa poput VoIP-a i ostalih audio tipova, video sadržaja, streaming-a, a također i tradicionalnih sadržaj poput IP podataka preko AP.

Podešavanje WMM QoS Parametara

WMM Settings

☑ Enable WMM ☐ Enable APSD ☐ Enable DLS

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Apply Change Reset Close

- **AC tip**

  Redovi čekanja, dodijeljeni prioriteti i parametri za prijenos su slijedeći:

  - **Data 0 (Best Effort, BE):** Srednji prioritet reda čekanja, srednja propusnost i kašnjenje. Tradicionalni IP podaci nalaze se u ovom redu čekanja.
  - **Data 1 (Background, BK):** Najmanji prioritet reda čekanja, velika propusnost. U ovom redu čekanja nalaze se podaci koji zahtijevaju maksimalnu propusnost i nisu vremenski osjetljivi (na primjer: FTP podaci).
  - **Data 2 (Video, VI):** Visoki prioritet reda čekanja. U ovaj rad, šalju se podaci osjetljivi na vrijeme poput video sadržaja i ostalih streaming medija koja zahtijevaju minimalno kašnjenje.
  - **Data 3 (Voice, VO):** Visoki prioritet reda čekanja, minimalno kašnjenje. Vremenski osjetljivi podaci poput VoIP-a automatski se šalju u ovaj red.

  Paketi koji se nalaze u redu čekanja većeg prioriteta prenijeti će se prije paketa koji se nalaze u redu čekanja manjeg prioriteta.

- **ECWmin i ECWmax**

  Ako pristupna točka otkrije da se koristi određeni mediji, upotrijebiti će *DCF random backoff timer* za određivanje vremena čekanja do slijedećeg pokušaja pristupa kanalu. Svaka pristupna točka čeka određeni period prije ponovnog pokušaja.

Vrijeme čekanja – slučajno definirana vrijednost unutar ranga definirana kao *Minimum Contention Window* eksponencijalno se povećava do definiranog limita *Maximum Contention Window.*

Slučajna čekanja – izbjegavaju većinu kolizija koje se mogu pojaviti ako višestruki AP u isto vrijeme imaju pristup mediju i istovremeno pokušavaju poslati podatke. Što je više aktivnih korisnika u vašoj mreži, to će veću ulogu imati *backoff timer* u poboljšanje performansi, smanjenu nastanka kolizija i ponovnog slanja.

Slučajni *backoff* kojeg koristi pristupna točka može se podesiti. Za opis slučajnog čekanja definirani su "*Minimum Contention Window" (ECWMin*) i "*Maximum Contention Window" (ECWMax)*.

- **ECWmin**: definirana vrijednost u *Minimum Contention Window* polju predstavlja gornji limit za inicijalno *backoff* vrijeme čekanja. Broj koji se koristi za slučajni *backoff* je slučajno odabran i nalazi se u rasponu između 0 i definiranog broja u polju *Minimum Contention Window.*
- **ECWmax**: Ukoliko prvo slučajno *backoff* vrijeme istekne prije nego se prenese podatkovni okvir, pristupna točka će povećati brojač i udvostručiti vrijednost unutar slučajnog *backoff* polja. Definirana vrijednost u *Maximum Contention Window* polju predstavlja gornju granicu slučajnog *backoff* vremena. Udvostručenje vremena nastavlja se sve dok se podatkovni okvir ne prenese ili dok se dostigne definirana vrijednost u *Maximum Contention Window* polju.

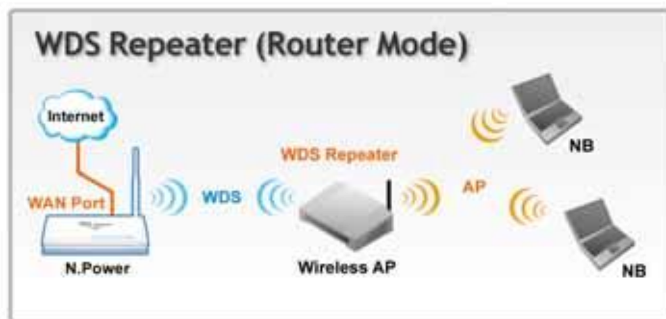
- **AIFS**
  Arbitration Inter-Frame Spacing (AIFs) definira vrijeme čekanja podatkovnih okvira (u milisekundama). 802.11e koristi međuokvirne razmake za reguliranje prava pristupa okvira slobodnim kanalima, a također se koristi i za koordiniranje vremena čekanja različitih tipova podataka. AIF osigurava da višestruke pristupne točke ne pokušavaju slati podatke u isto vrijeme, nego da umjesto toga čekaju dok kanal ne bude slobodan. AIF se definira u granicama od 1 do 255.

- **Transmission Opportunity (prilika za prijenos)**
  Transmission Opportunity (TXOP) je vremenski interval kada WMM klijentske stanice imaju pravo započeti prijenos preko bežičnog medija. Definirana vrijednost (u milisekundama) predstavlja vremenski interval kada WMM klijentske stanice imaju pravo započeti prijenos preko bežične mreže.



Preporučuje se upotreba standardnih postavki na WMM QoS stranici. Promjena vrijednosti može dovesti do neočekivanog blokirana prometa u bežičnoj mreži koje će biti teško dijagnosticirati.

4.4.10 WDS postavke (Repetitor)



Poznata kao WDS repetitor funkcija. Omogućavanje opcije dopušta udaljenom AP opremljenom s WDS funkcijom pojačanje bežičnog signala N. Power uređaja. Na N.Power uređaj mogu se spojiti četiri WDS repetitora. WDS radi na način da se unese MAC adresa (poznata kao BSSID) udaljene pristupne točke.

WDS Settings

WDS Mode

AP1 EncrypType NONE
Encryp Key
MAC Address

AP2 EncrypType NONE
Encryp Key
MAC Address

AP3 EncrypType NONE
Encryp Key
MAC Address

AP4 EncrypType NONE
Encryp Key
MAC Address

Apply Change | Close

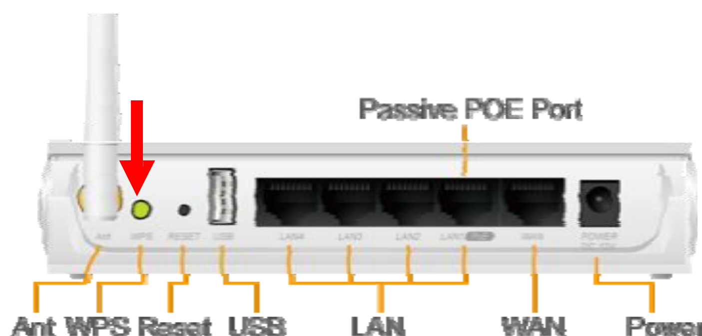
- **Encryp Type:** Možete koristiti jedan od četiri enkripcijska tipa:
  - **None:** Nema enkripcije. Nije preporučljivo pošto može prouzročiti ozbiljne sigurnosne propuste.
  - **WEP:** Najkompaktniji tip, ali i najlakši za probiti. Koristite ovu vrstu zaštite samo ako AES ili TKIP ne radi.
  - **TKIP:** Temporal Key Integrity Protocol, TKIP je sigurniji od WEP-a, ali manje sigurniji od AES-a.

- **AES:** Najsigurnija metoda šifriranja. Krajnje je preporučljivo koristiti ju u svim mogućim uvjetima.
- **Encryp Key:** Polje za unos enkripcijskog ključa.
- **MAC Address:** Unesite MAC adresu ili BSSID udaljenog premosnika. MAC adresu uređaja možete pronaći na naljepnici udaljenog premosnika.

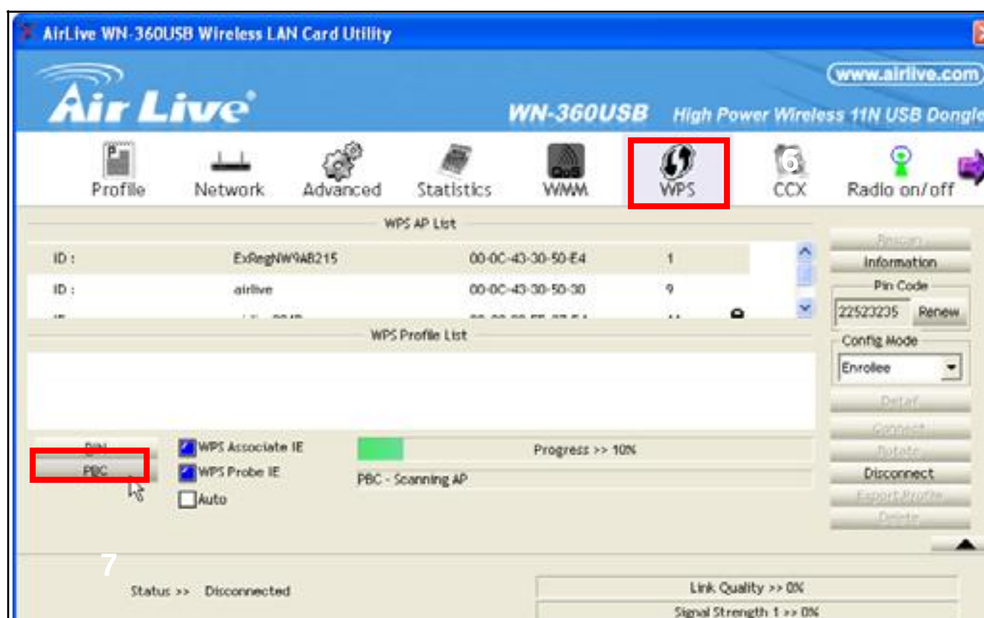
4.4.11 WPS postavke

Primjer 1: Pomoću hardverskog prekidača

Pritisnite WPS prekidač na poleđini N.Power uređaja. Nakon što WPS LED lampica počne svijetliti, N.Power uređaj početi će pretraživati klijentske WPS signale u okolini.
Unutar **dvije minute** morate uključiti pomoćni program vaše bežične mrežne kartice i kliknuti na PBC za automatsko spajanje.

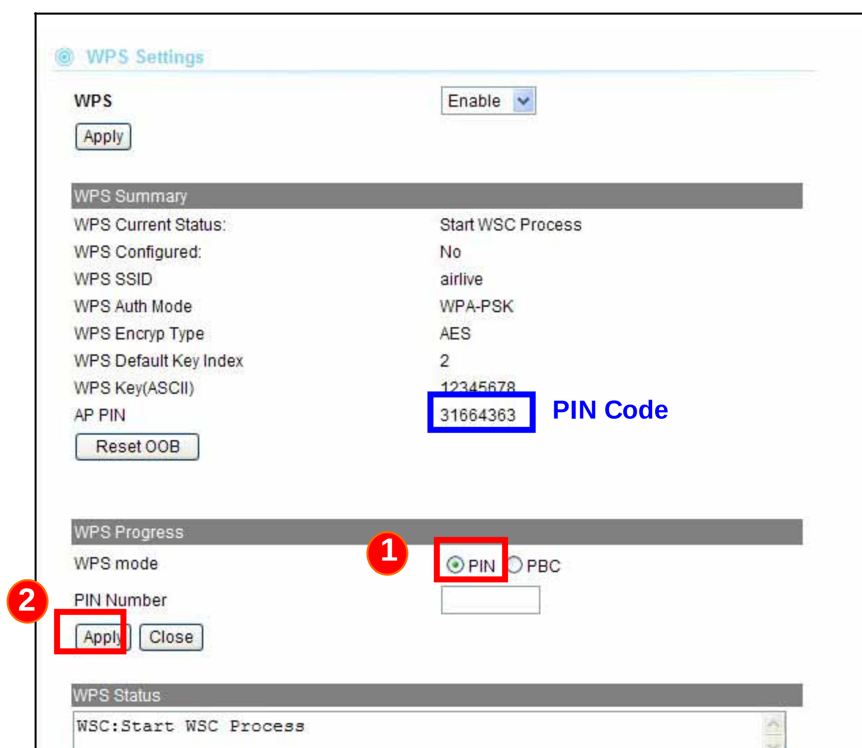


Ako imate WPS prekidač na bežičnoj kartici možete ga odmah pritisnuti, a ako nemate WPS funkciju možete pronaći u bežičnom pomoćnom programu. Ispod je primjer korištenja AirLive WN-360USB bežične mrežne kartice i spajanje na N.Power uređaj.

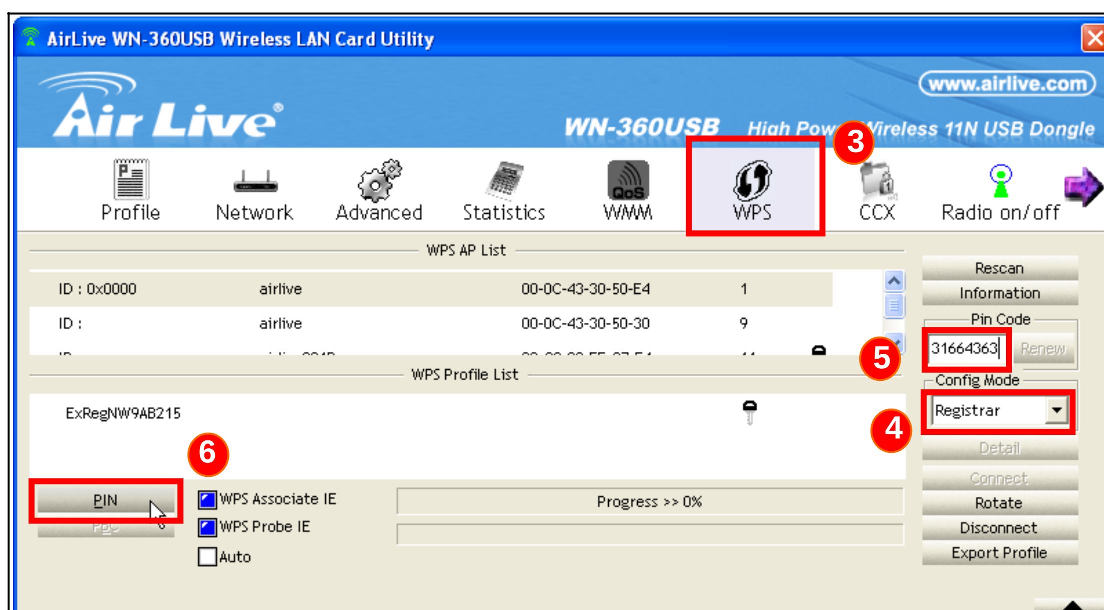


Primjer 2: WPS pomoću PIN-a

Prijavite se na N.Power web korisničko sučelje. Odaberite Wireless *Settings* -> *WPS Settings*. U *WPS Progress* dijelu odaberite „PIN“ i kliknite na „Apply“ za dobivanje PIN-a.



Zatim uključite pomoćni program bežične kartice, postavite WPS način na „*Registrar*“ i unesite PIN Code. Pritisnite PIN i veza će se automatski konfigurirati.


AirLive WN-360USB Wireless LAN Card Utility
www.airlive.com
WN-360USB
Profile
Network
Advanced
Statistics
WMM
WPS
CCX
Radio on/off
WPS AP List
ID : 0x0000
airlive
00-0C-43-30-50-E4
1
ID :
airlive
00-0C-43-30-50-30
9
WPS Profile List
ExRegNW9AB215
Rescan
Information
Pin Code
31664363
Renew
Config Mode
Registrar
Detail
Connect
Rotate
Disconnect
Export Profile
PIN
WPS Associate IE
WPS Probe IE
Auto
Progress >> 0%
3
4
5
6

5 Konfiguracija sustava i statusne informacije

U ovom poglavlju objasniti ćemo *System Configuration* (konfiguraciju sustava) i *Status Menu* (statusne informacije) web upravljačkog sučelja. Prije toga obavezno pročitajte Poglavlje 3.

5.1 Struktura izbornika

Kada kliknete na *System Configuration* izbornik u gornjem dijelu izbornika, pojaviti će se naredni prozor. Konfiguracija sustava uključuje sve postavke osim bežičnih postavki i one će biti objašnjene u nastavku.

5.2 Postavke LAN sučelja

System Configuration>> LAN Interface Setup

U ovom izborniku možete konfigurirati sve postavke vezane uz LAN sučelje uključujući IP adrese, DHCP poslužitelj postavke i slično.

LAN Interface Setup

You may enable/disable networking functions and configure their parameters as your wish.

IP postavke uređaja

Device IP Settings:

IP Address	192.168.1.254
Subnet Mask	255.255.255.0

DHCP postavke

DHCP Settings:

DHCP Type	Server
Start IP Address	192.168.1.100
End IP Address	192.168.1.200
Lease Time(sec)	86400

Static DHCP Client:

MAC Address	
Lease IP Address	

Add | Delete Selected | Delete All

Current static Lease Clients

MAC Address	Lease IP	Select

Apply Change | Cancel

5.2.1 DHCP postavke

- **DHCP Service:** Omogućavanje ili onemogućavanje DHCP poslužitelja.
  - **Disable**: Onemogući DHCP poslužitelj. Standardno DHCP poslužitelj je onemogućen u AP, klijentskom i WDP premosnom načinu rada.
  - **Server**: N.Power uređaj ponašati će se kao DHCP poslužitelj te će dodijeliti IP adrese klijentima koji se nalaze u LAN/bežičnom okruženju. Standardno DHCP poslužitelj je omogućen u usmjerivačkom radu.
- **DHCP Client Range**: Možete definirati raspon IP adresa u kojem će DHCP klijenti dobiti adrese. Kliknite na „Show Clients“ za prikaz trenutne DHCP tablice klijenata.
- **Lease Time:** Možete definirati vrijeme koliko dugo će N.Power rezervirati IP adrese za određeno računalo ili mrežne uređaje.

5.2.2 Dodavanje DHCP statičkih adresa

Ako želite vezati IP adrese za MAC adresu, trebate dodati DHCP klijente u *Static DHCP Client* tablicu. Možete unijeti do 40 klijenata. Ispod je opisana procedura za dodavanje unosa:

1. Unesite MAC adresu uređaja

2. Unesite IP adresu uređaja

3. Kliknite na "Add" gumb za dodavanje zapisa

Static DHCP Client:

MAC Address

Lease IP Address

Add | Delete Selected | Delete All

Current static Lease Clients

MAC Address	Lease IP	Select

Apply Change | Cancel

5.3 Podešavanje vremena

System Configuration ->Time Settings

Interno vrijeme N.Power uređaja možete postaviti na dva načina. Prvi način je ručno unošenje vremena, a drugi je pomoću NTP poslužitelja. Preporučuje se unos postavki putem NTP poslužitelja jer će sinkronizirati vrijeme čak i nakon nestanka struje.

- **Sync with Host**: Za sinkroniziranje vremena klijenta i poslužitelja.
- **Time Zone**: Odaberite grad najbliže vama.
- **NTP Server**: Lokacija NTP poslužitelja s kojim će se N.Power sinkronizirati.
- **NTP Synchronization**: Definiranje vremena koliko često će se N.Power sinkronizirati s udaljenim NTP poslužiteljom.

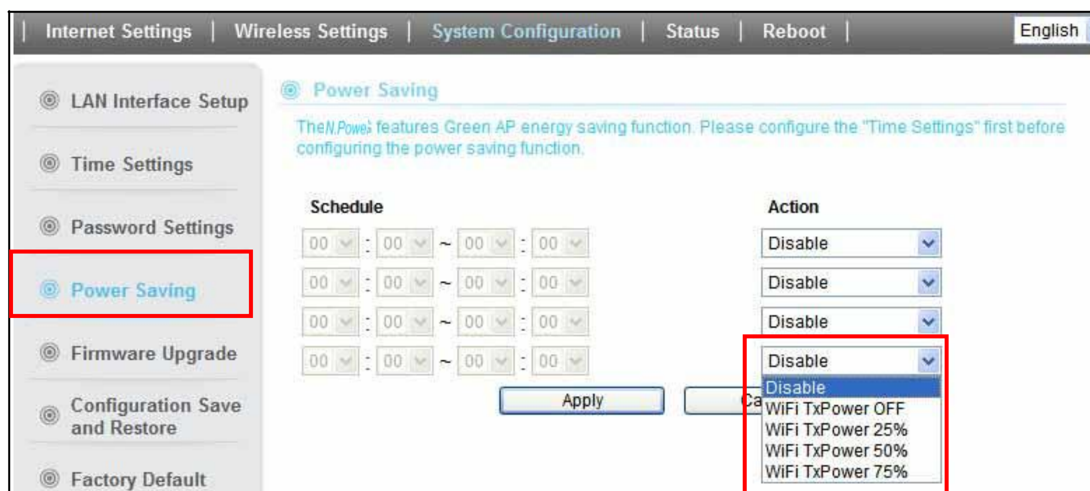
Kada napravite promjene, kliknite na gumb „Apply".

5.4 Postavke zaporke

System Configuration -> Password Settings
Korisničko ime i zaporku možete promijeniti na način prikazan na donjem prozoru.

5.5 Ušteda energije (Zeleni AP)

System Configuration -> Power Saving
Funkcija rasporeda ušteda energije omogućuje korisnicima definiranje vremena rada pristupne točke i jačine izlazne snage. Funkcija se koristi za uštedu energije zelenim radom vašeg AP.



5.6 Nadogradnja firmvera

System Configuration -> Firmver Upgrade

Firmver N.Power uređaja moguće je nadograditi (firmver je softver koji kontrolira rad N.Power uređaja). Nadogradnja firmvera radi se kada je dostupna nova verzija koja nudi nove mogućnosti ili rješava probleme u trenutnoj verziji.



- Nadogradnja firmvera
  Prvo preuzmite firmvare s AirLive web portala lokalno na računalo. Na gorenjem ekranu prikazan je prozor u kojem odaberete firmver s računala (kliknite *Browse* za pronalazak firmvera). Kliknite „Apply" za početak nadogradnje.

Novi firmver će se učitati u vaš N.Powe uređaj. Kada primite poruku o završetku nadogradnje, ponovno pokrenite uređaj. Tek nakon ponovnog pokretanja novi firmver će biti aktivan.



Nemojte isključivati uređaj za vrijeme nadogradnje. Nadogradnja novog firmvera preporuča se samo ukoliko nudi nove mogućnosti ili rješava probleme s trenutnim firmverom.

5.7 Spremanje konfiguracije i vraćanje postavki

System Configuration -> Configuration Save and Restore

N.Power ima opciju izvoza i uvoza konfiguracijskog dokumenta.

N.Power može sačuvati postavke u datoteci i kasnije ih po potrebi vratiti iz nje.

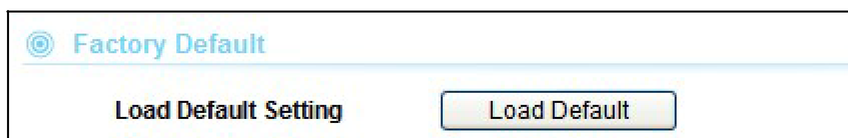
- **Export Settings:** Izvozi konfiguracijske podatke na računalo tako da kasnije možete povratiti staro stanje.
- **Import Settings file location:** Locirajte konfiguracijsku datoteku za vraćanje postavki.



5.8 Standardne tvorničke postavke

System Configuration -> Factory Default

Za učitavanje standardnih tvorničke postavki na N.Power uređaj.



5.9 Statusne informacije

5.9.1 Informacije o uređaju

Iz ovog izbornika možete saznati verziju firmvera, vrijeme koliko je sustav aktivan, IP i MAC adrese i provjeriti da li je spojen USB spremnik.

Device Information

Internet	
Firmware Version	v27.4.2.0.1-b2
System Up Time	0day:0h:5m:23s
Operation Mode	WDS Bridge Mode
Local Network	
Local IP Address	192.168.7.7
Local Netmask	255.255.255.0
MAC Address	00:0C:43:30:50:77
DHCP Type	DHCP Server OFF
WDS	
Status	NONE
USB Information	
Product Name	No USB device plug-in.

5.9.2 Statistike

Statistički prozor prikazuje status memorije, WAN, LAN i WLAN promet.

Statistic

Take a look at the statistics about system.

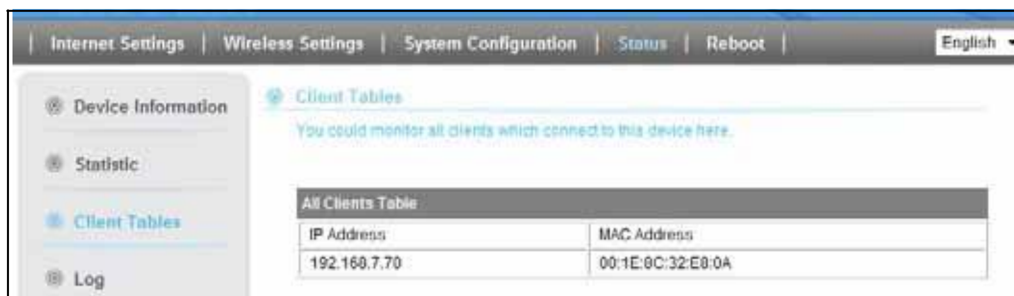
Memory	
Memory Total	28956 kB
Memory Left	8256 kB

WAN/LAN	
WAN Rx Packets	1211
WAN Rx Bytes	103993
WAN Tx Packets	337
WAN Tx Bytes	198008
LAN Rx Packets	1212
LAN Rx Bytes	103993
LAN Tx Packets	337
LAN Tx Bytes	198008

WLAN	
WLAN Rx Packet	2394
WLAN Rx Byte	185569
WLAN Tx Packet	1395
WLAN Tx Byte	211608

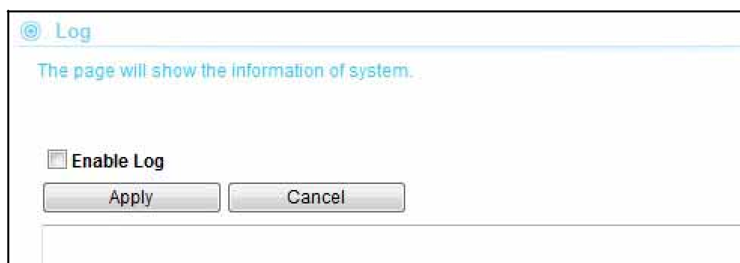
5.9.3 Tablica klijenata

Tablica klijenata poznata je još pod nazivom ARP tablica. Prikazuje sve IP i MAC adrese uređaja koji prolaze kroz N.Power uređaj.



5.9.4 Zapisi

Kada omogućite log funkciju, sustav će spremati sve zapise o događajima i greškama.



6 AP način

U ovom poglavlju objasniti ćemo bežične postavke za AP način. Prije toga pročitajte Poglavlje 1.4 i Poglavlje 3.

6.1 AP način

Kada N.Power uređaj radi u pristupnom načinu, ponaša se kao centralni koncentrator bežične mreže. Svi bežični uređaji i klijenti komuniciraju kroz N.Power uređaj. Ovakva vrsta mreže poznata je pod nazivom „Infrastrukturna mreža“. Ostali N.Power ili 802.11 b/g/n uređaji mogu se spojiti na AP kroz klijentski način.

AP Mode
NB
N.Power
NB
NB

6.2 Bežične postavke

Wireless Settings

Wireless Interface	Enable
Regulatory Domain	ETSI (Europe)
Network ID (SSID)	airlive ☐ Hide SSID
Multiple SSID	Setup
Channel	Auto
Radio Mode	11b/g/n
Wireless Security	Setup
Client Isolation	○ Enable ◉ Disable
Tx Output Power	About 17dBm
Access Control	Setup
Associated Clients	Setup
Advance Settings	Setup
WMM Settings	Setup
WDS Settings	Setup
WPS Settings	Setup

Apply Change | Reset

6.2.1. Regulacijska tijela

Wireless Settings -> Regulatory Domain

Regulacijsko tijelo određuju koji kanali i koja razina Tx izlazne snage je dostupna u vašoj zemlji. U većini slučajeva domena je ispravno postavljena. Korištenje neispravne domene strogo je zabranjeno. Ako živite u Europi morate koristiti ETSI regulatorsku domenu, a ako živite u SAD-u morate koristiti FCC domenu.

N.Power je usklađen s narednim regulacijskim tijelima:

Regulacijsko tijelo	Dostupni kanali	Maksimalna Tx izlazna snaga
ETSI (Europa)	1 ~13	20dBm
FCC (SAD)	1~11	23dBm
Južna Amerika (11 CH)	1~11	30dBm
Južna Amerika (14 CH)	1~14	30dBm

6.2.2 Višestruki SSID

Wireless Settings -> Multiple SSID

Višestruki SSID dopušta kreiranje maksimalno 4 različite bežične mreže (SSID). Ta funkcija poznata je pod nazivom *Virtual AP*. Svaki SSID može imati svoju politiku šifriranja. SSID1 je glavna bežična mreža unutar *Wireless Settings* stranice.

- **Hide SSID**: Bežična mreža postati će nevidljiva te će biti dostupna samo osobama koji znaju naziv SSID-a.
- **Enable Isolation between SSIDs**: Uključivanje opcije onemogućiti će promet između različitih bežičnih mreža.

6.2.3 Kanali

Wireless Settings -> Channel

Kanal predstavlja frekvencijski rang za prijenos signala. U 802.11 g/b standardu postoji maksimalno 14 kanala. Međutim, dostupnost kanala u svakoj zemlji ovisi o lokalnim regulacijama. Ako živite u Europi, možete koristiti kanale od 1 do 13, a ako živite u SAD-u onda možete koristiti kanale od 1 do 11.

Wireless Settings

Wireless Interface — Enable
Regulatory Domain — FCC (United States)
Network ID (SSID) — airlive — Hide SSID
Multiple SSID — Setup
Channel — Auto
Radio Mode
Wireless Security
Client Isolation
Tx Output Power
Access Control
Bandwidth Control
Associated Clients
Advance Settings
WMM Settings — Setup
WDS Settings — Setup
WPS Settings — Setup

Auto
2412MHz (Channel 1)
2417MHz (Channel 2)
2422MHz (Channel 3)
2427MHz (Channel 4)
2432MHz (Channel 5)
2437MHz (Channel 6)
2442MHz (Channel 7)
2447MHz (Channel 8)
2452MHz (Channel 9)
2457MHz (Channel 10)
2462MHz (Channel 11)

Apply Change — Reset

6.2.4 Bežična zaštita

Wireless Settings -> Wireless Security

Preporučljivo je odmah postaviti bežičnu zaštitu i osigurati siguran prijenos podataka i spriječiti neovlašteni pristup. **Najlakši način za postavljanje zaštite je pomoću čarobnjaka *Setup Wizard*. Čarobnjak automatski odabire najsigurniju i najlakšu shemu za zaštitu vaše bežične mreže.** Ukoliko želite sami postaviti sigurnosnu zaštitu, N. Power nudi različite enkripcijske modele poput: WEP, WPA-PSK, WPA, WPA2, WPA2-PSK. Općenito, WPA-PSK i WPA2-PSK su najpopularnije i najsigurnije metode zaštite.

Procedura postavljanja zaštite



- **Korak 1**: **Select your SSID:** Ako ste omogućili „Multiple SSID" u padajućem izborniku pojaviti će mogućnost odabira različitog SSID-a. Svaki SSID (Virtualni AP) može imati vlastitu politiku zaštite.
- **Korak 2**: **Odabir „Security Policy"**: N.Power nudi široki raspon sigurnosnih politika uključujući: WEP (Pre-Shared Key), WPA (certificate), WPA-PSK (AES), WPA2-PSK (AES) i 802.1x *Radius Authentication*. Nedavno su WiFi regulacije zabranile korištenje TKIP enkripcije u 11n standardu te je TKIP dostupan samo u 11 b/g standardu. Preporučuje se upotreba WPA-PSK AES sigurnosnog protokola kao najjednostavnijeg i najsigurnijeg načina zaštite.

6.2.5 Kontrola pristupa

Wireless Settings -> Access Control

N.Power omogućuje definiranje liste MAC adresa koje imaju mogućnost pristupa mreži ili kojima je zabranjen pristup bežičnoj mreži. Funkcija je dostupna samo u AP i AP usmjerivačkom načinu rada.



- **Disable:** Onemogućuje MAC filtriranje.

- **Allow list:** Kada se odabere, podatkovni promet u mreži biti će dopušten samo navedenim uređajima u tablici.

- **Deny list:** Kada se odabere, podatkovni promet u mreži biti će zabranjen samo navedenim uređajima u tablici.

6.2.6 Tablica klijenata

Wireless Settings -> Associated Client

Status bežičnih klijenata možete provjeriti u tablici ispod.

Client Tables

You could monitor stations which associated to this AP here.

Associated Clients

MAC Address	Power Saving	Modulation	Channel Width	RSSI(dB)	Time(Sec)
00-0C-43-30-50-80	0	7	40M	-61	58

Close

- **MAC Address**: MAC adresa bežičnih klijenata. Ako želite pronaći IP adresu, pogledajte pod *Status -> Client Table* izbornik.
- **Power Saving**: **0**: Ušteda energije je isključena. **1**: Ušteda energije je uključena.
- **Modulation**: Prikazuje koji MCS nivo se koristi u 11n načinu.
- **Channel Width**: Definira da li klijent koristi 20MHz ili 40MHz širinu kanala.
- **RSSI (dBm)**: Snaga signala klijentskog uređaja.
- **Time (Sec)**: Koliko je dugo vremena je spojen bežični klijent.

6.2.7 Napredne postavke

Wireless Settings -> Advance Settings

- **Channel Width:** Možete odabrati širinu kanala od 20 MHz ili 20/40 Mhz. Odaberite 20 MHz zbog sukladnosti sa zakonom u nekim državama. 40 MHz nudi bolje performanse od 20 MHz.

- **Guard Interval**: *Guard interval* nalazi se na početku svakog prijenosa. Koristi se za smanjenje efekta miješanja višestrukih putanja prijenosa. Korištenje dugog *Guard Intervala* može smanjiti miješanje u višestrukom okruženjima, ali zato može smanjiti performanse.
- **MCS (Modulation and Code Scheme):** MCS nivo za 11n standard. Preporuča se ostaviti postavku na Auto.

Advance Setup

Channel BandWidth	○ 20 ◉ 20/40
Guard Interval	○ long ◉ Auto
MCS	Auto
Decline BA Request	◉ Disable ○ Enable
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	○ Enable ◉ Disable
Short Slot	◉ Enable ○ Disable
Tx Burst	◉ Enable ○ Disable
Pkt Aggregate	◉ Enable ○ Disable
TX ACK Timeout	32 usec
RX ACK Timeout	10 usec
Calculate ACK Timeout value	Calculate
Multicast-to-Unicast	○ Enable ◉ Disable

Apply Change   Close

- **Decline BA Request:** Omogućite opciju za odbijanje *Block ACK* zahtjeva od drugih uređaja.

- **BG Protection:** 802.11g standard uključuje mehanizam zaštite koji pružaju zajednički rad 802.11b i 802.11g standarda. Ukoliko nema takovog mehanizma, dvije vrste standarda mogu se međusobno miješati i smanjiti mrežne performanse.

- **Beacon Interval:** Uređaj redovito emitira ispitne poruke da bi obznanio svoju postojanost. Ispitna poruka (Bacon Interval) definira koliko često se ispitna poruka prenosi u jedinici vremena u milisekundama. Standardna vrijednost je 100, a ispravna vrijednost trebala bi biti između 1 i 65.535.

- **Fragmentation: K**ada veličina *unicast* poruke pređe fragmentacijski prag, onda će biti fragmentirna prije prijenosa. Trebala bi imati vrijednost od 356 do 2346 bajtova, sa standardnom vrijednosti 2346. Ukoliko se pojave visoki novo pogrešno prenesenih paketa, trebali bi smanjiti fragmentacijski prag.

- **RTS Threshold:** RTS/CTS okviri koriste se za kontrolu medija za prijenos. Sve *unicast* poruke (podaci ili kontrola) veće od definiranog RTS praga, mogu se prenijeti nakon RTS/CTS mehanizma razmijene. RTS prag bi trebao imati vrijednost između 256-2347 bajta, dok je standardna vrijednosti **2347**. Ne preporuča se preveliko odstupanje od standardne veličine.

- **Short Preamble**: Preambula je signal koji se koristi u bežičnom okruženju za sinkroniziranje vremena prijenosa pomoću *Synchronization* i *Start* okvirnog graničnika. U „bučnim" mrežnim okolinama, tip preambule trebao bi biti postavljen na dugu preambulu (Long Preambule). Kratka preambula (Short Preambule) koristi se kod aplikacija koje su minimalno zahtjevne i koje traže maksimalne performanse. U „bučnom" mrežnom okruženju, performanse će se smanjiti.

- **Tx Burst and Packet Aggregate:** Postoje sheme za poboljšanje performansi prijenosa podataka u 11n i Turbo standardima. Preporučljivo je omogućiti ove opcije.

- **AckTimeOut:** Kada bežična stanica pošalje paket prema drugoj bežičnoj stanici, čekati će na potvrdi okvir (Acknowledgement Frame) od nje. Stanica će čekati samo određeno vrijeme, a to vrijeme se zove *ACK timeout*. **Standardne vrijednosti Tx i Rx *timeout-a* su točne u većini slučajeva te njihove vrijednosti nije potrebno mijenjati.**

6.2.8 WMM postavke

Wireless Settings -> WMM Settings

Wi-Fi Multimedia (WMM) je standard za prioritiziranje multimedijalnih aplikacija. WMM postavke služe za podešavanje višestrukih redova čekanja za postizanje boljih performansi različitih bežičnih paketa poput VoIP-a i ostalih audio tipova, video sadržaja, streaming-a, a također i tradicionalnih sadržaj poput IP podataka preko AP.

Air Live

Podešavanje WMM QoS parametara

WMM Settings

☑ Enable WMM ☐ Enable APSD ☐ Enable DLS

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Apply Change Reset Close

- **AC tip**

  Redovi čekanja, dodijeljeni prioriteti i parametri za prijenos su slijedeći:

  - **Data 0 (Best Effort, BE):** Srednji prioritet reda čekanja, srednja propusnost i kašnjenje. Tradicionalni IP podaci nalaze se u ovom redu čekanja.
  - **Data 1 (Background, BK):** Najmanji prioritet reda čekanja, velika propusnost. Podaci koji zahtjevaju maksimalnu propusnost i nisu vremenski osjetljivi nalazi se u ovom redu čekanja (na primjer: FTP podaci).
  - **Data 2 (Video, VI):** Visoki prioritet reda čekanja. Podaci osjetljivi na vrijeme poput video sadržaja i ostalih streaming medija koja zahtijevaju minimalno kašnjenje automatski se šalju u ovaj red.
  - **Data 3 (Voice, VO):** Visoki prioritet reda čekanja, minimalno kašnjenje. Vremenski osjetljivi podaci poput VoIP-a automatski se šalju u ovaj red.

  Paketi koji se nalaze u redu čekanja većeg prioriteta prenijeti će se prije nego paketi koji se nalaze u redu čekanja manjeg prioriteta.

- **ECWmin i ECWmax**

  Ako pristupna točka otkrije da se koristi određeni mediji, upotrijebiti će *DCF random backoff timer* za određivanje vremena čekanja do slijedećeg pokušaja pristupa kanalu. Svaka pristupna točka čeka određeni period prije ponovnog pokušaja.

Vrijeme čekanja – slučajno definirana vrijednost unutar ranga definirana kao *Minimum Contention Window*, eksponecijalno se povećava do definiranog limita *Maximum Contention Window.*

Slučajna čekanja – izbjegavaju većinu kolizija koje se mogu pojaviti ako višestruki AP u isto vrijeme imaju pristup mediju i istovremeno pokušavaju poslati podatke. Što je više aktivnih korisnika u vašoj mreži, to će veću ulogu imati *backoff timer* u poboljšanje performansi, smanjenu nastanka kolizija i ponovnog slanja.

Slučajni *backoff* kojeg koristi pristupna točka može se podesiti. Za opis slučajnog čekanja definirani su *Minimum Contention Window (ECWMin*) i *Maximum Contention Window (ECWMax)*.

- **ECWmin**: definirana vrijednost u *Minimum Contention Window* polju predstavlja gornji limit za inicijalno *backoff* vrijeme čekanja. Broj koji se koristi za slučajni *backoff* je slučajno odabran i nalazi se u rasponu između 0 i definiranog broja u polju *Minimum Contention Window.*
- **ECWmax**: Ukoliko prvo slučajno *backoff* vrijeme istekne prije nego se prenese podatkovni okvir, pristupna točka će povećati brojač i udvostručiti vrijednost unutar slučajnog *backoff* polja. Definirana vrijednost u *Maximum Contention Window* polju predstavlja gornju granicu slučajnog *backoff* vremena. Udvostručenje vremena nastavlja se sve dok se podatkovni okvir ne prenese ili dok se dostigne definirana vrijednost u *Maximum Contention Window* polju.

o **AIFS**

Arbitration Inter-Frame Spacing (AIFs) definira vrijeme čekanja podatkovnih okivra (u milisekundama). 802.11e koristi međuokvirne razmake za reguliranje prava pristupa okvira slobodnim kanalima, a također se koristi i za koordiniranje vremena čekanja različitih tipova podataka. AIF osigurava da višestruke pristupne točke ne pokušavaju slati podatke u isto vrijeme, nego da umjesto toga čekaju dok kanal ne bude slobodan. AIF se definira u granicama od 1 do 255.

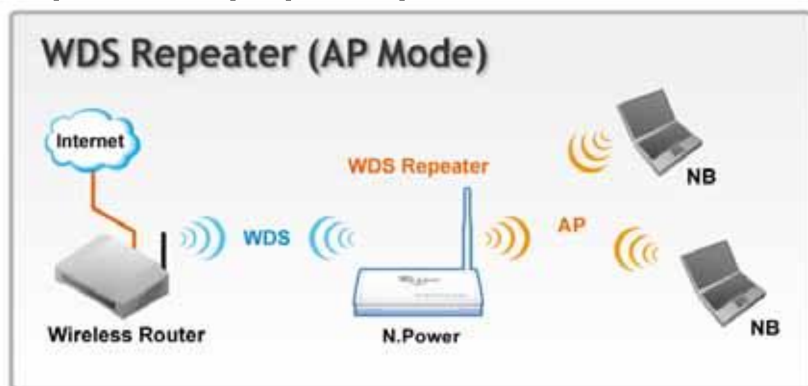
o **Transmission Opportunity – prilika za prijenos**

Transmission Opportunity (TXOP) je vremenski interval kada WMM klijentske stanice imaju pravo započeti prijenos preko bežičnog medija. Definirana vrijednost (u milisekundama) predstavlja vremenski interval kada WMM klijentske stanice imaju pravo započeti prijenos preko bežične mreže.



Preporučuje se upotreba standardnih postavki na WMM QoS stranici. Promjena vrijednosti može dovesti do neočekivanog blokiranja prometa u bežičnoj mreži koje će biti teško dijagnosticirati.

6.2.9 WDS postavke (Repetitor)



Poznata kao WDS repetitor funkcija. Omogućavanje opcije dopušta udaljenom AP opremljenom s WDS funkcijom pojačanje bežičnog signala N. Power uređaja. Na N.Power uređaj mogu se spojiti četiri WDS repetitora. WDS radi na način da se unese MAC adresa (poznata kao BSSID) udaljene pristupne točke.

WDS Settings

☐ WDS Mode

AP1 EncrypType NONE
Encryp Key
MAC Address

AP2 EncrypType NONE
Encryp Key
MAC Address

AP3 EncrypType NONE
Encryp Key
MAC Address

AP4 EncrypType NONE
Encryp Key
MAC Address

Apply Change Close

- **Encryp Type:** Možete koristiti jedan od četiri enkripcijska tipa:
  - **None:** Nema enkripcije. Nije preporučljivo pošto može prouzročiti ozbiljne sigurnosne propuste.
  - **WEP:** Najkompaktniji tip, ali i najlakši za probiti. Koristite ovu vrstu zaštite samo ako AES ili TKIP ne radi.

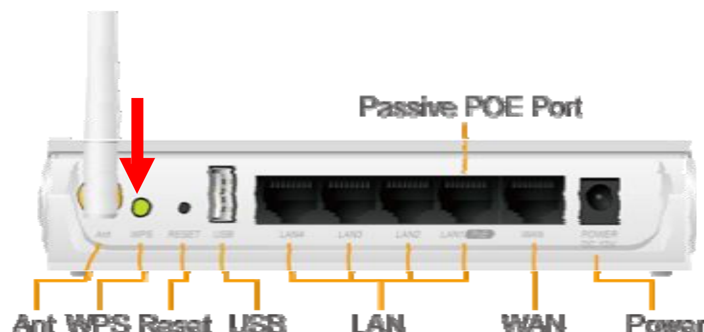
- **TKIP:** Temporal Key Integrity Protocol, TKIP je sigurniji od WEP-a, ali manje sigurniji od AES-a.
- **AES:** Najsigurnija metoda šifriranja. Krajnje je preporučljivo koristiti ju u svim mogućim uvjetima.

- **Encryp Key:** Unesite enkripcijski ključ.
- **MAC Address:** Unesite MAC adresu ili BSSID udaljenog premosnika. MAC adresu uređaja možete pronaći na naljepnici udaljenog premosnika.

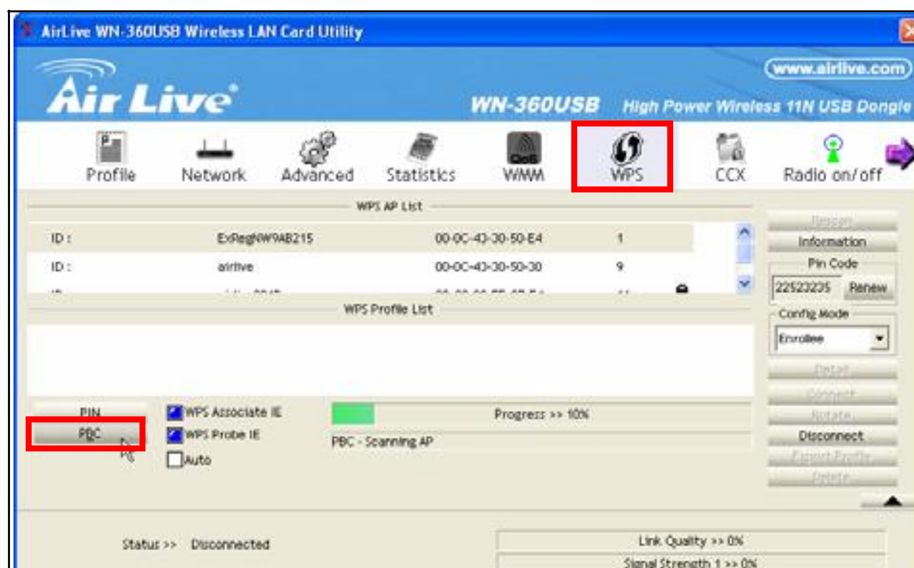
6.2.10 WPS Postavke

Primjer 1: Pomoću hardverskog prekidača

Pritisnite WPS prekidač na poleđini N.Power uređaja. Nakon što WPS LED lampica počne svijetliti, N.Power uređaj početi će pretraživati klijentske WPS signale u okolini.
Unutar **dvije minute** morate uključiti pomoćni program vaše bežične mrežne kartice i kliknuti na PBC za automatsko spajanje.

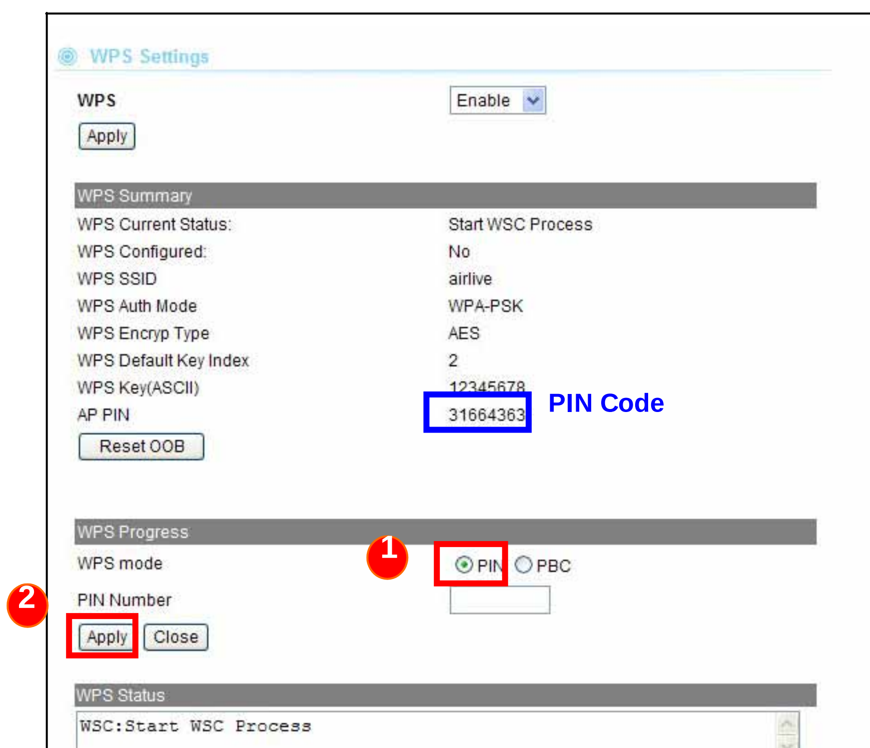


Ako imate WPS prekidač na bežičnoj kartici možete ga odmah pritisnuti, a ako nemate WPS funkciju možete pronaći u bežičnom pomoćnom programu. Ispod je primjer korištenja AirLive WN-360USB bežične mrežne kartice i spajanje na N.Power uređaj.

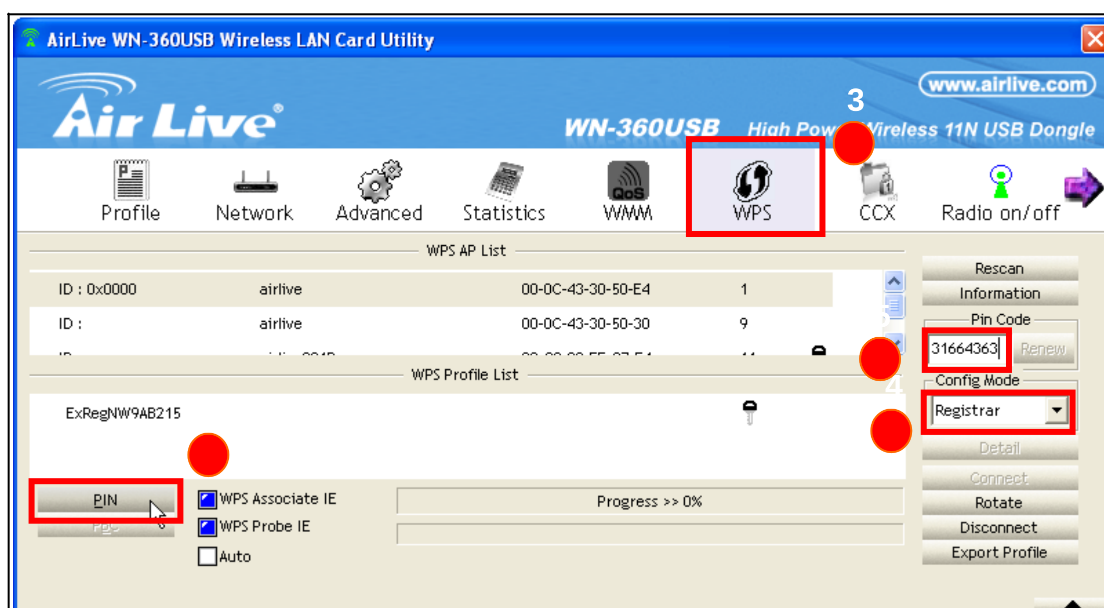


Primjer 2: WPS pomoću PIN-a

Prijavite se na N.Power web korisničko sučelje. Odaberite Wireless *Settings* -> *WPS Settings*. U *WPS Progress* dijelu odaberite PIN i kliknite na „Apply“ za dobivanje PIN-a.



Zatim uključite pomoćni program bežične kartice, postavite WPS način na „*Registrar*“ i unesite *PIN Code*. Pritisnite PIN i veza će se automatski konfigurirati.



7 Klijentski način

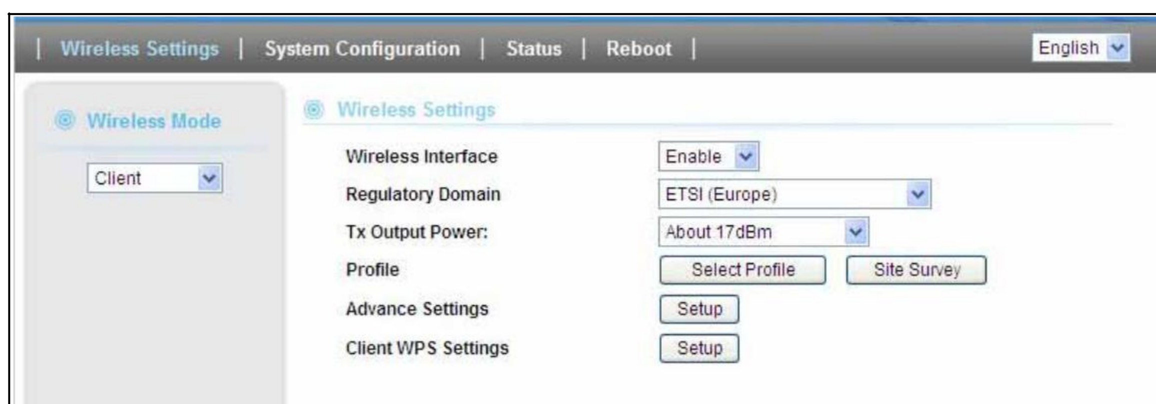
U ovom poglavlju objašnjen je klijentski način rada N.Power uređaja. Prije toga pročitajte Poglavlje 1.4 i Poglavlje 3.

7.1 Klijentski način

Ovaj način rada poznat je pod nazivom „Client mode“. N.Power ponaša se kao bežični uređaj koji se spaja na pristupnu točku. Za mrežni pristup korisnik može spojiti računalo ili usmjerivač na LAN port N.Power uređaja.



7.2 Bežične postavke



7.2.1 Regulacijsko tijelo

Wireless Settings -> Regulatory Domain

Regulacijsko tijelo određuje koji kanali i koja razina Tx izlazne snage je dostupna u vašoj zemlji. U većini slučajeva domena je ispravno odabrana. Korištenje neispravne domene strogo zabranjeno. Ako živite u Europe morate koristiti ETSI domenu, a ako živite u SAD-u morate koristiti FCC domenu.

N.Power je usklađen s narednim regulacijskim tijelima:

Regulacijsko tijelo	Dostupni kanali	Maksimalna Tx izlazna snaga
ETSI (Europa)	1 ~13	20dBm
FCC (SAD)	1~11	23dBm
Južna Amerika (11 CH)	1~11	30dBm
Južna Amerika (14 CH)	1~14	30dBm

7.2.2 Postavke profila

Wireless Settings -> Profile Setting

Profil sadrži informacije o udaljenoj AP mreži. Unutar klijentskog načina rada možete odabrati dvije metode za spajanje s udaljenom pristupom točkom.

1. Pomoću *Site Survay* opcije možete pronaći AP na koji se želite spojiti i zatim odabrati SSID za spajanje. Ovo je najlakši način.

2. Možete kreirati profil na koji AP se želite spojiti. Procedura je objašnjena u nastavku.

Procedura dodavanja profila

1. Kliknite na „Profile Setting" u *Wireless Setting* izborniku. Zatim kliknite na „Add" za dodavanje novog profila.



2. Na stranici za dodavanje profila, unesite informacije o udaljenoj pristupnoj točki poput SSID-a i načina zaštite. Kada ste završili kliknite na „Apply“.

Add Profile

Profile Name	PROF001
SSID	airlive
Network Type	Infrastructure
Power Saving Mode	CAM (Constantly Awake Mode) / Power Saving Mode
RTS Threshold	Used 2347 (range 1 - 2347, default 2347)
Fragment Threshold	Used 2346 (range 256 - 2346, default 2346)
Security Mode	WPA2-Personal
WPA Algorithms	TKIP AES
Pass Phrase	•••••••••••• (8~63 ASCII or 64 HEX characters)

Apply Cancel

3. Kada ste potvrdili kreiranje novog profila, trebao bi se pojaviti na listi. Odaberite ga i kliknite na „Activate“ gumb za primjenu postavki. Samo jedan profil može istovremeno biti aktivan.

Profile Setting

Pofile List

	Profile	SSID	Channel	Authentication	Encryption	Network Type
	PROF001	airlive	Auto	WPA2-PSK	AES	Infrastructure
	PROF002	airlive2	Auto	WPA-PSK	TKIP	Infrastructure

Add Delete Edit Activate Close

7.2.3 Site Survey

Wireless Settings -> Site Survey

Bežične mreže oko vas možete skenirati koristeći funkciju *Site Survey*. *Site Survey* funkcija pruža mogućnost podešavanja antene i uspostavu bežične veze.

Kada kliknete na *Site Survey* gumb, pojaviti će se naredni prozor. Osvježavanje prozora može potrajati ovisno o dostupnim pristupnim točkama u okolini.

Site Survey

SSID	SSID	BSSID	RSSI	Channel	Encryption	Authentication
◉	LU3G	00-0C-43-30-50-EC	-96 dbm	1	AES	WPA2-PSK
○	WT2K	00-4F-67-00-61-BA	-86 dbm	10	TKIP	WPA-PSK
○		00-12-0E-92-D7-E3	-94 dbm	9	TKIP	WPA2-PSK
○	airlive301R	00-C0-02-FF-C7-E4	-98 dbm	11	AES	WPA2-PSK

Connect Rescan Close

Možete odabrati SSID na koji se želite spojiti i pritisnuti „Connect“ gumb. U slučaju da je postavljena zaštita, pojaviti će se prozor za unos enkripcijskih pristupnih podataka.

7.2.4 Napredne postavke

Advance Settings

Wireless Mode(Infra) 11b/g/n
BG Protection Mode Auto
TX ACK Timeout 32 usec
RX ACK Timeout 10 usec
Calculate RF ACK Timeout value Calculate
Tx Burst

HT Physical Mode
Channel BandWidth 20 Auto
Guard Interval Long Auto
MCS Auto

Apply Change Close

- **BG Protection:** 802.11g standard uključuje mehanizam zaštite koji pruža zajednički rad 802.11b i 802.11g standarda. Ukoliko nema takovog mehanizma, dvije vrste standarda mogu se međusobno miješati i smanjiti mrežne performanse.

- **AckTimeOut:** Kada bežična stanica pošalje paket prema drugoj bežičnoj stanici, čekati će na potvrdi okvir (*Acknowledgement Frame*) od nje. Stanica će čekati samo određeno vrijeme, a to vrijeme se zove *ACK timeout*. **Standardne vrijednosti Tx i Rx *timeout-a* su u većini slučajeva točne te njihove vrijednosti nije potrebno mijenjati.**

- **Tx Burst:** Sheme koje se koriste za poboljšanje performansi kod prijenosa podataka kod 11n standarda. Preporuča se ostaviti omogućenu opciju.

- **Channel Width:** Možete odabrati širinu kanala od 20 MHz ili 20/40 Mhz. Odaberite 20 MHz zbog sukladnosti sa zakonom u nekim državama. 40 MHz nudi bolje performanse od 20 MHz.

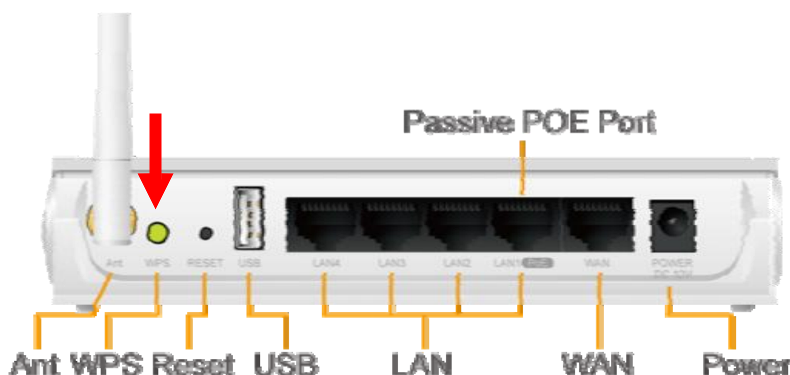
- **Guard Interval**: *Guard interval* nalazi se na početku svakog prijenosa. Koristi se za smanjenje efekta miješanja višestrukih putanja prijenosa. Korištenje dugog *Guard Intervala* može smanjiti miješanje u višestrukom okruženjima, ali zato može smanjiti performanse.

- **MCS (Modulation and Code Scheme):** MCS nivo za 11n standard. Preporuča se ostaviti postavku na Auto.

7.2.5 WPS postavke

Primjer 1: Pomoću hardverskog prekidača

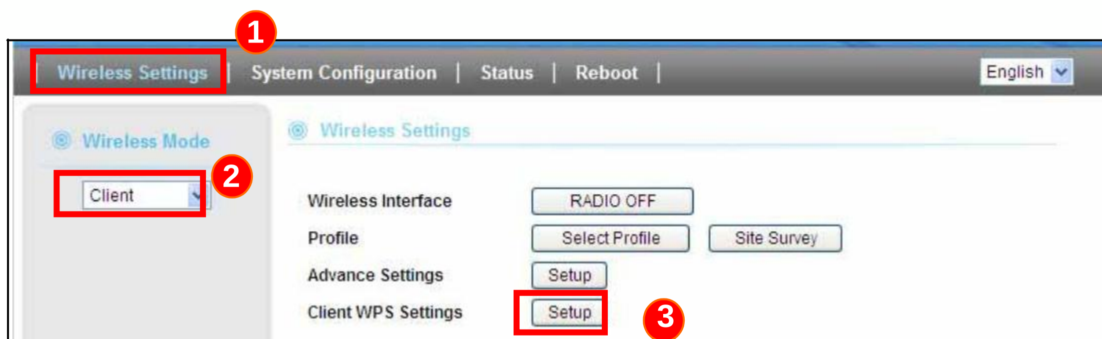
Pritisnite WPS prekidač na poleđini N.Power uređaja. Nakon što WPS LED lampica počne svijetliti, N.Power uređaj početi će pretraživati klijentske WPS signale u okolini.



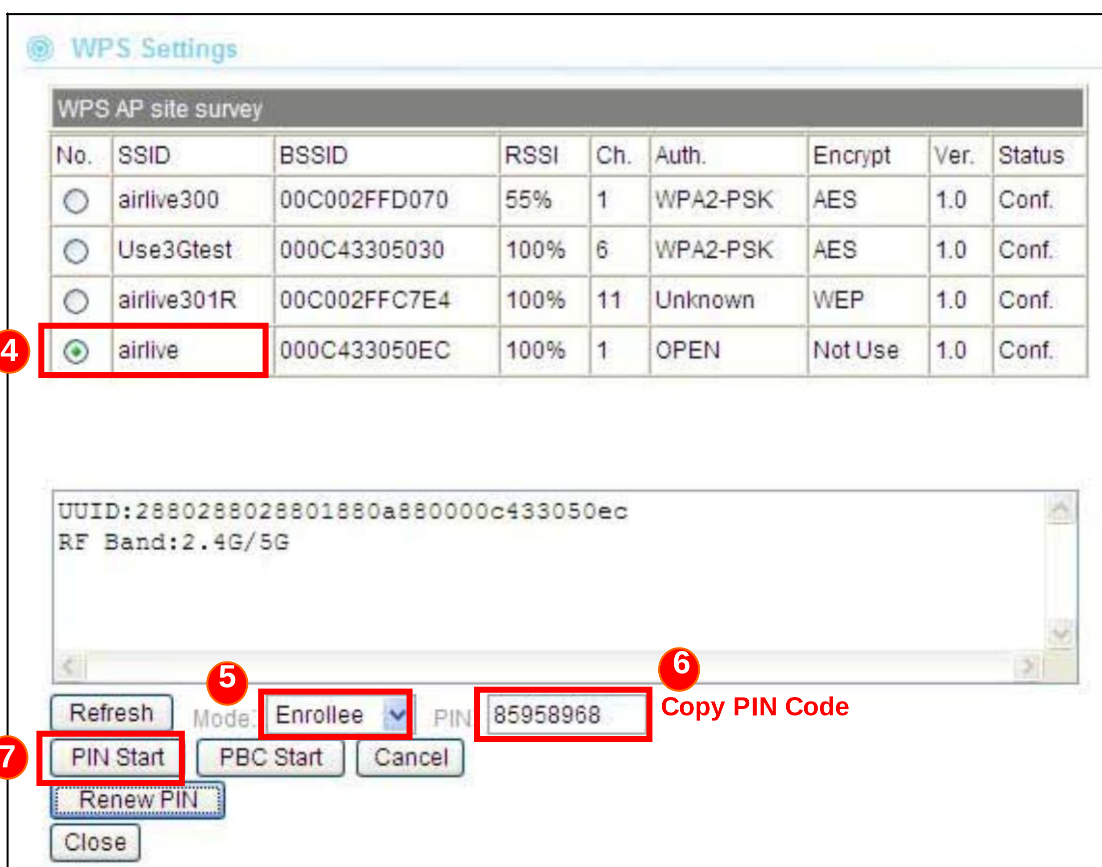
Unutar **dvije minute** morate uključiti pomoćni program vaše bežične mrežne kartice i kliknuti na PBC za automatsko spajanje.

Primjer 2: WPS pomoću PIN-a

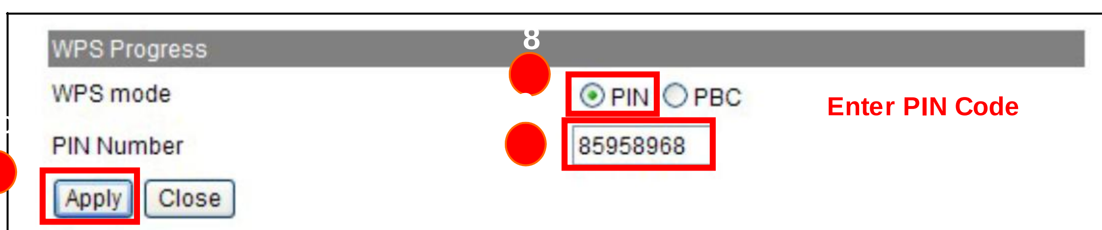
Prijavite se na N.Power web korisničko sučelje. Odaberite *Wireless Settings -> WPS Settings*. U *WPS Progress* dijelu odaberite PIN i kliknite na „Apply“ za dobivanje PIN-a.



Odaberite SSID na koji se želite spojiti. Postavite WPS način na *Enrollee* i tada ćete dobiti PIN kod. Pritiskom na „PIN Start" WPS LED dioda će dvije minute svijetliti na uređaju.



Pod AP stranicom odaberite *Wireless Setting -> WPS Setting*. Postavite WPS način na PIN, unesite pin kod i kliknite na „Apply" za automatski uspostavljanje veze.



WPS Settings

WPS AP site survey

No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
◉	DlinkOwen	001B11E4DA95	10%	3	WPA-PSK; WPA2-PSK	TKIP; AES	1.0	Conf.
○	TiMotion	001E5833E567	5%	3	WPA-PSK; WPA2-PSK	TKIP; AES	1.0	Conf.

```
UUID:7aa25ee77d0336b4a114e14323f4842a
Primary Device Type:Unknown:1536,1266
```

Refresh Mode: Enrollee PIN: 31662567

PIN Start PBC Start Cancel

Renew PIN

Close

WPS Status

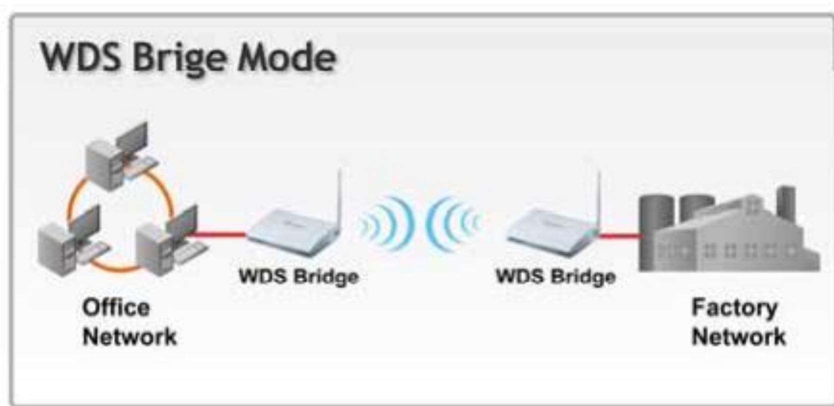
```
Not used
```

8 WDS premosni način

U ovom poglavlju objasniti ćemo bežične postavke za WDS Bridge (premosnik) način. Prije toga pročitajte Poglavlje 1.4 i Poglavlje 3.

8.1 WDS premosni način rada

Ovaj način rada poznat je pod nazivom *„WDS Pure MAC Bridge mode“.* Svaki premosnik može se povezati s maksimalno 4 ostala premosnika. Način rada najčešće se koristi kada želimo bežično povezati LAN mreže (na primjer: mreže između ureda i skladišta). Način rada omogućuje bolje performanse nego infrastrukturni način.



8.2 Bežične postavke

Wireless Interface	Enable
Regulatory Domain	ETSI (Europe)
Channel	Auto
Radio Mode	11b/g/n
Tx Output Power	16.5 dBm (Index 10)
Advance Settings	Setup
WDS Settings	Setup
Apply Change	Reset

8.2.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

Regulacijsko tijelo određuju koji kanali i koja razina Tx izlazne snage je dostupna u vašoj zemlji. U većini slučajeva domena je ispravno odabrana. Korištenje neispravne domene strogo zabranjeno. Ako živite u Europi morate koristiti ETSI domenu, a ako živite u SAD-a morate koristiti FCC domenu.

N.Power je usklađen s narednim regulacijskim tijelima:

Regulacijsko tijelo	Dostupni kanali	Maksimalna Tx izlazna snaga
ETSI (Europa)	1 ~13	20dBm
FCC (SAD)	1~11	23dBm
Južna Amerika (11 CH)	1~11	30dBm
Južna Amerika (14 CH)	1~14	30dBm

8.2.2 Napredne postavke

Wireless Settings -> Advance Setup

Advance Setup

Channel BandWidth	○ 20 ◉ 20/40
Guard Interval	○ long ◉ Auto
MCS	Auto
Decline BA Request	◉ Disable ○ Enable
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	○ Enable ◉ Disable
Short Slot	◉ Enable ○ Disable
Tx Burst	◉ Enable ○ Disable
Pkt Aggregate	◉ Enable ○ Disable
TX ACK Timeout	32 usec
RX ACK Timeout	10 usec
Calculate ACK Timeout value	Calculate
Multicast-to-Unicast	○ Enable ◉ Disable

Apply Change Close

- **Channel Width:** Možete odabrati širinu kanala od 20 MHz ili 20/40 Mhz. Odaberite 20 MHz zbog sukladnosti sa zakonom u nekim državama. 40 MHz nudi bolje performanse od 20 MHz.
- **Guard Interval**: *Guard interval* nalazi se na početku svakog prijenosa. Koristi se za smanjenje efekta miješanja višestrukih putanja prijenosa. Korištenje dugog *Guard Intervala* može smanjiti miješanje u višestrukom okruženjima, ali zato može smanjiti performanse.
- **MCS (Modulation and Code Scheme):** MCS nivo za 11n standard. Preporuča se ostaviti postavku na Auto.
- **Decline BA Request:** Omogućite opciju za odbijanje *Block ACK* zahtjeva od drugih uređaja.
- **BG Protection:** 802.11g standard uključuje mehanizam zaštite koji pruža zajednički rad 802.11b i 802.11g standarda. Ukoliko nema takovog mehanizma, može doći do interferencije između dva standardna i do smanjenja mrežnih performansi.
- **Beacon Interval:** Uređaj redovito emitira ispitne poruke da bi obznanio svoju postojanost. Ispitna poruka (Bacon Interval) definira koliko često ispitna poruka se prenosi u jedinici vremena u milisekundama. Standardna vrijednost je 100, a ispravna vrijednost trebala bi biti između 1 i 65.535.
- **Fragmentation:** Kada veličina *unicast* poruke pređe fragmentacijski prag, onda će biti fragmentirana prije prijenosa. Trebala bi imati vrijednost od 356 do 2346 bajtova, sa standardnom vrijednosti 2346. Ukoliko dođe do visoke razine pogrešno prenesenih paketa, trebali bi smanjiti fragmentacijski prag.
- **RTS Threshold:** RTS/CTS okviri koriste se za kontrolu medija za prijenos. Sve *unicast* poruke (podaci ili kontrola) veće od definiranog RTS praga, mogu se prenijeti nakon RTS/CTS mehanizma razmijene. RTS prag bi trebao imati vrijednost između 256-2347 bajta, dok je standardna vrijednost **2347**. Ne preporučuje se preveliko odstupanje od standardne veličine.
- **Short Preamble**: Preambula je signal koji se koristi u bežičnom okruženju za sinkroniziranje vremena prijenosa pomoću *Synchronization* i *Start* okvirnog graničnika. U „bučnim" mrežnim okolinama, tip preambule trebao bi biti postavljen na dugu preambulu (Long Preambule). Kratka preambula (Short Preambule) koristi se kod aplikacija koje su minimalno zahtjevne i koje traže maksimalne performanse. U „bučnom" mrežnom okruženju, performanse će se smanjiti.
- **Tx Burst and Packet Aggregate:** Postoje sheme za poboljšanje performansi prijenosa podataka u 11n i Turbo standardima. Preporučljivo je omogućiti ove opcije.

- **AckTimeOut:** Kada bežična stanica pošalje paket prema drugoj bežičnoj stanici, čekati će na potvrdi okvir (*Acknowledgement Frame*) od nje. Stanica će čekati samo određeno vrijeme, a to vrijeme se zove *ACK timeout*. **Standardne vrijednosti Tx i Rx *timeout-a* su u većini slučajeva točne te njihove vrijednosti nije potrebno mijenjati.**

8.2.3 WDS postavke

Kod premosnih mreža, potrebno je unijeti bežične MAC adrese svih premosnika koji su spojeni direktno na vaš N.Power uređaj. Bežična MAC adresa poznata je pod nazivom BSSID.

WDS Settings

AP1 EncrypType NONE
Encryp Key
MAC Address

AP2 EncrypType NONE
Encryp Key
MAC Address

AP3 EncrypType NONE
Encryp Key
MAC Address

AP4 EncrypType NONE
Encryp Key
MAC Address

Apply Change Close

- **Encryp Type:** Možete koristiti jedan od četiri enkripcijska tipa:
  - **None:** Nema enkripcije. Nije preporučljivo pošto može prouzročiti ozbiljne sigurnosne propuste.
  - **WEP:** Najkompaktniji tip, ali i najlakši za probiti. Koristite ovu vrstu zaštite samo ako AES ili TKIP ne radi.
  - **TKIP:** Temporal Key Integrity Protocol. TKIP je sigurniji od WEP-a, ali manje sigurniji od AES-a
  - **AES:** Najsigurnija metoda šifriranja. Krajnje je preporučljivo koristiti ju u svim mogućim uvjetima.

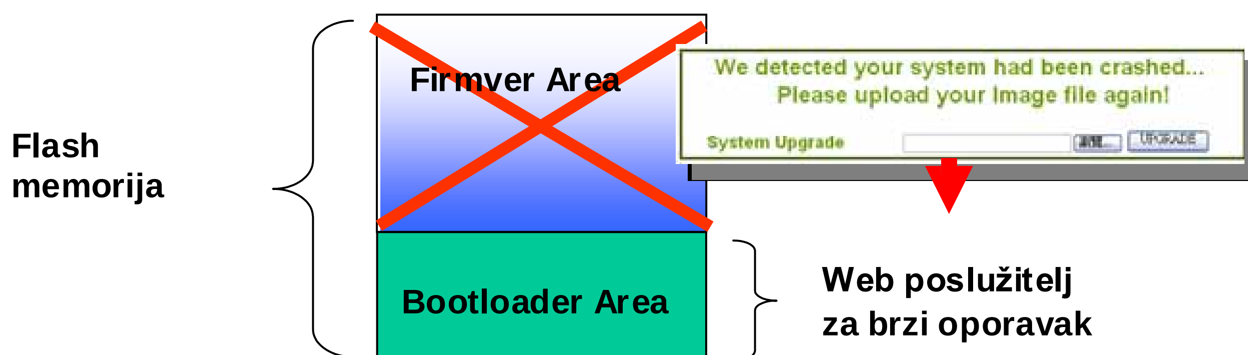
- **Encryp Key:** Unesite enkripcijski ključ.
- **MAC Address:** Unesite MAC adresu ili BSSID udaljenog premosnika. MAC adresu uređaja možete pronaći na naljepnici udaljenog premosnika.

9 Brzi oporavak firmvera

N.Power ima opciju brzog oporavka firmvera koja omogućuje vraćanje firmvera na AP u slučaju pada sustava. Ako ne može pristupiti AP-u, probajte povratiti postavke na standardne pritiskom RESET gumba (sa stražnje strane uređaja) duže od 10 sekundi. Nakon toga trebali bi moći pristupiti AP putem IP adrese 192.168.1.254. Ukoliko ne budete mogli pristupiti uređaju, pokrenite brzi oporavak firmvera. Posjetite www.airlive.com-> *support* -> *download* i upišite "N.Power".

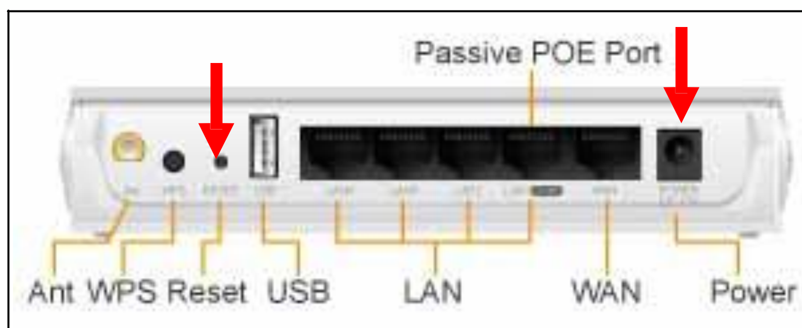
Kako funkcionira brzi oporavak?

N. Power flash memorija podijeljena je na „firmware" i „bootloader" područje. Bootloader područje je samo za čitanje i ima u sebi ugrađeni web poslužitelj za brzi oporavak, što omogućuje oporavak AP firmvera u slučaju pada sustava. Web poslužitelj za brzi oporavak pokrene se kada AP uđe u stanje brzog oporavka te će se njegova IP adresa promijeniti na ***192.168.1.254***.



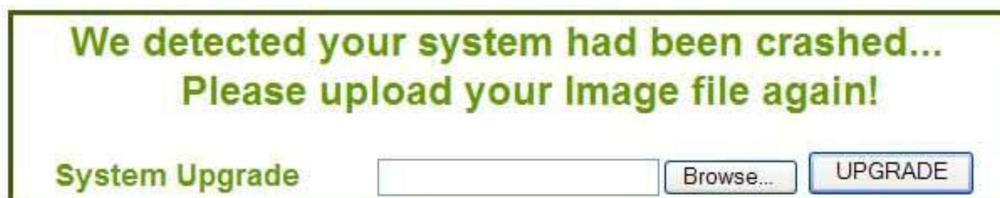
Procedura za vraćanje postavki AP koristeći brzi oporavak

1. Računalo direktno spojite na jedan od LAN portova (LAN1~LAN4).
2. Postavite IP adresu računala na 192.168.1.50.
3. Prije spajanja struje, pritisnite i držite „Reset" gumb (sa stražnje strane AP uređaja) i tada uključite napajanje. Držite „Reset" gumb dok se LED lampica odabranog porta ne upali (oko 3 sekunde).



Slika 1-2: Pritisnite i držite „Reset" gumb dok uključujete napajanje

6. Otvorite pretraživač i upišite 192.168.1.254. Naredni prozor će se pojaviti.



7. Kliknite na „Browse" gumb i otvorite ispravnu firmver datoteku.

8. Kliknite na „UPGRADE" gumb. Nemojte dirati AP ili računalo dok nadogradnja ne završi.



9. Nakon nadogradnje, konfiguracije će se nadograditi s prijašnjim postavkama. Pristupite uređaju preko **prijašnje IP adrese.** Ako ste zaboravili koja je prijašnja IP adresa uređaja, pritisnite i držite „Reset" gumb duže od 10 sekundi za vraćanje tvorničkih postavki. Sustav će se ponovno pokrenuti. Sada bi se trebali moći normalno prijaviti na web sučelje putem standardne IP adrese: 192.168.1.254.

.

10 Učestala pitanja

U ovom poglavlju prikazana su neka učestala pitanja o N.Power uređaju

Pitanje: Uključio sam USB spremnik u N.Power uređaj, ali nije prepoznat

Odgovor:
1. Provjerite da li ste uključili USB spremnik na ispravnu stranu.
2. Provjerite da li vaš USB spremnik koristi FAT ili FAT32 format. NTFS nije podržan.
3. Ako koristite USB tvrdi disk, trebate spojiti vanjski adapter za napajanje.

===

Pitanje: Nakon brze nadogradnje ne mogu pronaći N.Power na adresi 192.168.1.254

Odgovor: N.Power povratiti će prijašnje postavke nakon uspješnog brzog oporavka. Zbog toga će se IP adresa promijeniti na IP adresu koju ste prije koristili. Ako ni u tom slučaju ne možete naći N.Power uređaja, vratite tvorničke postavke na standarde. N.Power uređaj trebao bi se pojavit na IP adresi 192.168.254.

==

Pitanje: Kada koristim *Site Survey* funkciju na spajanje na pristupnu točku koja ne koristi zaštitu, zašto N.Power uređaj izbaci pogrešku „encryption type mismatch!“ i traži me podešavanje bežičnih sigurnosnih postavki?

Odgovor: Kada kliknete na „Connect“ sa *Site Survey* stranice, N.Power će prvo provjeriti da li su trenutne bežične sigurnosne postavke ispravne. Ako nisu, tražiti će vas da promijenite postavke. Zbog toga, ukoliko vaše trenutne bežične postavke sadrže enkripciju, a novi AP na koji se želite spojiti ne koristi zaštitu, tada će N.Power prijaviti nepodudaranje. U tom slučaju jednostavno kliknite na „Disable“ u enkripcijskom polju u pritisnite „Apply Change“.

==

Pitanje: Kada promijenim bežični radni način, zašto više ne mogu pronaći AP?

Odgovor: DHCP poslužitelj je standardno omogućen u usmjerivačkom načinu rada, dok je u ostalim načinima DHCP poslužitelj onemogućen. Ako automatski dobijete

IP adresu i tada promijenite s usmjerivačkog rada na AP / klijentski / WDS premosni način, vaše računalo više neće moći dobiti IP adresu od DHCP poslužitelja. U tom slučaju trebate ručno postaviti IP adresu.

==

Pitanje: Gdje se nalazi PoE port za N.Power uređaj?

Odgovor: PoE sustav koji se koristi kod N.Power uređaja je 12V pasivni PoE. LAN1 se koristi kao pasivni PoE port.

==

Pitanje: Kada koristim PoE napajanje s USB spremnikom, zašto ponekad nastanu problemi u radu?

Odgovor: Koristite 12VDC strujno napajanje koje podržava više od 1,25A.

==

Pitanje: Zašto PoE prespojnik ne radi kada ga spojim s N.Power uređajem?

Odgovor: N.Power koristi 12V pasivni PoE sustav koji nije isti kao i 48V sustav kojeg koristi PoE prespojnik. Štoviše, spajanje 48V sustava na N.Power uređaj može oštetiti vaš uređaj.

==

Pitanje: N.Power koristi 30 dBm izlazne snage, zašto onda vidim samo 20 dBm na opciji *Tx Output Power*?

Odgovor: Maksimalna izlazna snaga na konektoru za antenu je 1 vat (30 dBm). Međutim, zbog regulacija i usklađenosti u Europi izlazna snaga je limitirana na 20 dBm, a u SAD na 23 dBm. Uobičajeni usmjerivaču pružaju manje od 15 dBm izlazne snahe u 11n standardu, dok N.Power omogućuje do 19 dBm (Europa) i 22 dBm (SAD) u 11n standardu što omogućuje veliku pokrivenost u 11n standardu. Ako živite u državama koje dopuštaju 30 dBm izlazne snage, možete promijeniti regulatorske postavke na South America (Južna Amerika). Korištenje neispravnih regulacija je nedopušteno i može biti kažnjivo.

==

Pitanje: N.Power se reklamira kao uređaj s 2 vata (30 dBm) izlazne snage. Zašto se vidi samo 1 vat (30dBm) u web sučelju?

Odgovor: Maksimalno 2 vata predstavlja kombinaciju izlazne snage N.Power uređaja i 3 dBi antene.

11 Specifikacije

Specifikacija N.Power uređaja je podložna promjenama bez objave. Koristite informacije s oprezom.

11.1 Mogućnosti hardvera

11.1.1 Općenite mogućnosti hardvera

- Bežični-NAT usmjerivač velikog dometa
- Do 30 dBm izlazne snage (20 dBm u EU, 23 dBm u SAD)
- Do 9 puta veća bežična pokrivenost nego ostali AP/usmjerivači
- 1 x USB 2.0 port za FTP dijeljenje datoteka
- Zelena AP funkcija uštede energije
- 150Mb/s 1T1R bežični-b/g/n standard
- 12V pasivni POE Port
- WAN port za širokopojasni pristup Internetu
- Usmjerivački, AP, klijentski, premosni i repetitorski način rada
- Višestruki SSID i kontrola propusnosti
- 8MB Flash, 32MB SDRAM

11.1.2 Napajanje

- Voltaža napajanja : ulaz 100~240Vac/50~60Hz, izlaz 12V/1A
- Pasivni PoE port (prima 12Vdc). Pasivni PoE DC ubrizgivač nije uključen

11.1.3 Dimenzije i težina

- Dimenzije: 154 x 130 x 316 mm
- AP težina (okvirno): 280g
- Težina paketa (okvirno): 686g

11.2 Specifikacije signala

11.2.1 Širina frekvencijskog pojasa

- USA (SAD) (FCC) 11 kanala: 2.412GHz~2.462GHz
- Europe (Europa) (ETSI) 13 kanala: 2.412GHz~2.472GHz
- South America (Južna Amerika): 11 kanala: 2.412GHz~2.462GHz
- South America (Južna Amerika): 14 kanala: 2.412GHz~2.477GHz

11.2.2 Modulacije i frekvencije

- Frekvencije:
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 i 6 Mb/s
  - 802.11b: 11, 5.5, 2 i 1 Mb/s

- Modulacije:
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 i 6 Mb/s
  - 802.11b: 11, 5.5, 2 i 1 Mb/s

11.2.3 TX izlazna snaga

ETSI (Europa)

- 802.11b : Oko 20 dBm maksimalno
- 802.11g : Oko 20 dBm maksimalno
- 802.11n : Oko 19 dBm maksimalno

FCC (SAD)

- 802.11b : Oko 23 dBm maksimalno
- 802.11g : Oko 23 dBm maksimalno
- 802.11n : Oko 22 dBm maksimalno

South America (Južna Amerika)

- 802.11b : Oko 30dBm maksimalno
- 802.11g : Oko 29dBm maksimalno
- 802.11n : Oko 27dBm maksimalno

11.2.4 Osjetljivost prijemnika

- 802.11b 11Mb/s -90 dBm
- 802.11g 54Mb/s -73 dBm
- 802.11n HT20 MCS7 -70 dBm
- 802.11n HT40 MCS7 -67 dBm

11.2.5 Podržani WLAN načini

- Usmjerivački način
- AP način
- Klijentski način
- WDS premosni način
- WDS repetitorski način

11.3 Mogućnosti softvera

Upravljačko sučelje

- Web HTTP

Napredne funkcije

- Čarobnjak za postavke
- *Site Survey* – traženje stranica
- FTP dijeljenje datoteka
- Kontrola propusnosti / kontrola prometa
- Tablica klijenata
- Wi-Fi, WPA kompatibilna interoperabilnost
- WPA s PSK/TKIP/AES podrškom, WPA2 podrška
- Funkcija virtualnog poslužitelja
- Podržana odvojena privatnost
- Podržano sakrivanje SSID-a

- Podržano konfiguriranje izlazne snage
- ACK Timeout podešavanje
- Bootloader zaštita i brzi oporavak firmver koda
- Podržan Radius
- Statički DHCP unosi
- Firmver nadogradnja i postavljanje sigurnosne kopije putem web-a

12 Rječnik

Rječnik sadrži objašnjene pojmove pojedinih izraza. Možda su pojedine informacije u rječniku zastarjele, zato ih koristite s oprezom.

802.3ad
802.3ad je IEEE standard za spajanje višestrukih Ethernet portova u jedan virtualni port (poznate pod nazivom *truncking*) radi povećanja propusnosti.

802.3af
802.3af je PoE (Power over Ethernet) IEEE standard. 803.af koristi 48V PoE standard koji radi do 100 metara udaljenosti.

802.11b
Međunarodni standard za bežično povezivanje koje radi u 2.4 GHz frekvencijskom rangu (2,4 GHz do 2.4835 GHz) i omogućuje propusnost do 11 Mb/s.

802.1d STP
Spanning Tree Protocol je protokol koji služi za formiranje mreže. STP protokol omogućuje kreiranje redundantne veze u slučaju pada određene veze. Preporučljivo je uključiti opciju za kreiranje višestruko-povezane premosne mreže.

802.11d
Poznat pod nazivom "Global Roaming". 802.11d standard koristi se u zemljama u kojima su ostali standardi iz 802.11 grupe zabranjeni za upotrebu.

802.11e
802.11e je IEEE QoS standard za prioritiziranje VoIP-a i prometa multimedijalnih aplikacija. WMM je baziran na podvrsti 802.11e standarda.

802.11g
Standard koji omogućuje propusnost do 54 Mb/s uz pomoć OFDM tehnologije. Također radi u 2.4GHz frekvencijskom rangu isto kao i 802.11b standard. 802.11g uređaji kompatibilni su s 802.11b uređajima.

802.11i
IEEE standard za bežičnu sigurnost. 802.11i standard uključuje TKIP, CCMP i AES enkripcije za poboljšanje sigurnosti. Također je poznat kao WPA2.

802.1x
802.1x je sigurnosni standard za žičane i bežične LAN mreže. U 802.1x standardu uobičajeno postoje *supplicant* (kllijent), *authenticator* (prespojnik ili AP) i autentifikacijski poslužitelj (radius poslužitelj). Kada klijent zatraži servis, *autheticator* će proslijediti zahtjev i čekati odgovor od autetifikacijskog poslužitelja da dopusti pristup i registrira račun. 802.1x je najrasprostranjenija metoda za autetifikaciju kod WISP-a.

Adhoc

Peer-to-Peer bežične mreže. Adhoc bežične mreže ne koriste bežični AP ili usmjerivač kao centralni koncentrator u mreži, nego su umjesto toga klijenti spojeni direktno jedan na drugog. Nedostatak Adhoc mreža je manjak žičanih sučelja prema internet vezama. Ne preporuča se kreiranje mreže s više od dva čvora.

ACK Timeout
Acknowledgement Timeout Windows. Kada se paket pošalje s jedne bežične stanice na drugu, stanica će čekati određeno vrijeme na potvrdi okvir od udaljene stanice. Stanica će čekati samo određeno vrijeme i to vrijeme poznato je pod nazivom ACK timeout. Ako se ACK ne primi unutar definiranog vremena, paket će biti ponovno poslan što će rezultirati smanjenjem propusnosti. Ako je vrijeme čekanja na ACK okvir preveliko, tada propusnot neće biti iskorištena jer će se izgubiti vrijeme na čekanje potvrdnog okvira. Ako je vrijeme

čekanja na ACK okvir premalo, propusnost će biti smanjena zbog ponovnog slanja ispravnih paketa. S mogućnošću postavljanja ACK postavki, možete efektivno optimizirati propusnost na velike udaljenosti. To posebno dolazi do izražaja kod 802.11a i 802.11g mreža. Ispravno postavljanje ACK *timeout-a* ovisi o tri faktora: udaljenosti, vremenu odaziva pristupne točke i o smetnjama. N.Power nudi mogućnost ACK postavljanje na temelju udaljenosti ili direktnim unosom. Kada unesete udaljenost, N.Power će automatski izračunati ispravnu vrijednost ACK *timeout*-a.

Bootloader

Bootloader je osnovni program koji će se pokrenuti za vrijeme paljenja prije nego uređaj pokrene firmver. Sličan je BIOS-u na osobnom računalu. Kada dođe do prestanka rada firmvera, možete ga povratiti iz bootloader-a.

CPE uređaji

CPE (Customer Premises Equipment) je uređaj instaliran na korisničkoj strani za primanje mrežnih servisa. Na primjer: u ADSL mreži, ADSL modem/usmjerivač kod klijenta predstavlja CPE uređaj. Bežični CPE znači potpuni bežični uređaj (uobičajeno pristupna točka s ugrađenom antenom) koji prima bežični širokopojasni signal od WISP-a.

CTS

Clear To Send. Signal kojeg šalje uređaj kojim objavljuje da je spreman primiti podatke.

Čvor (Node)

Krajnja mrežna točka (računalo).

DDNS

Dynamic Domain Name System. Algoritam koji omogućuje upotrebu dinamičkih IP adresa za internet poslužitelje. DDNS servis omogućuje svakom korisniku račun s domenski imenom. Usmjerivač s DDNS mogućnostima ima ugrađenog DDNS klijenta koji ažurira IP informacije o promjeni IP adrese prema DDNS pružatelju usluga. DDNS omogućuje klijentu izradu web stranica na poslužitelju koji nema stalnu IP adresu.

DHCP
Dynamic Hosting Configuration Protocol. Protokol koji omogućuje automatsko dodjeljivanje IP adresa. Kada se računalo spoji na mrežu, ono automatski dobije IP adresu od DHCP poslužitelja. DHCP poslužitelj može biti određeno računalo u mreži ili drugi mrežni uređaj poput usmjerivača.

DMZ
Demilitarized Zone. Kada usmjerivač otvori DMZ port prema unutrašnjem mrežnom uređaju, on će prema njemu otvoriti sve TCP/UDP portove. Ova opcija se uobičajeno koristi kod postavljanja H.323 VoIP ili Multi-Media poslužitelja.

DNS
Prevodi URL u IP adrese na način da pristupa bazama podataka u kojima se nalazi popis internet poslužitelja.

Domena
Jedinstveno ime koje identificira internet stranicu. Domena se uvijek sastoji od dva ili više dijelova koji su odvojeni točkom. U www.airlive.com, "airlive.com" je ime domene.

DoS napad
Denial of Service. Vrsta mrežnog napada koja poplavi mrežu s nepotrebnim prometom. DoS napadi poput *Ping of Death* ili *Teardrop* napada, iskorištavaju ograničenja unutar TCP/IP protokola.

Enkripcija
Podaci se šifriraju radi sprečavanja čitanja bez ovlaštenog pristupa. Uobičajene bežične zaštite su WEP, WPA i WPA2.

ESSID (SSID)
Identifikacijsko ime 802.11 bežične mreže. Pošto bežična mreža nema fizičke barijere poput žičane Ethernet mreže, bežični LAN treba identifikator za razlikovanje mreža. Bežični klijeti moraju znati SSID za spajanje na WLAN. Opcije *Hide SSID* onemogućuje SSID emitiranje tako da korisnik mora znati SSID za spajanje na bežičnu mrežu.

Firmver
Program koji radi unutar uređaja poput usmjerivača ili pristupne točke. Većina mrežnih uređaja može nadograditi firmver putem web sučelja ili pomoćnih programa.

FTP
File Transfer Protocol. Standardni protokol za slanje datoteka između računala putem TCP/IP mreža i interneta.

Fragment Threshold (Fragmentirani prag)
Veličina okvira koja je veća nego *Fragmented Threshold* podijeliti će se u manje dijelove. Ako postoje smetnje u vašem području, manja postavljena vrijednost može poboljšati performanse. Ukoliko nema smetnji, ostavite parametar na velikoj vrijednosti. Standardna vrijednost je 2346. Kada postoje smetnje u vašoj mreži, možete probati postaviti vrijednosti na 1500, 1000 ili 500.

Mrežna vrata (Gateway)
Gledajući internet globalno, mrežna vrate predstavljaju centralne usmjerivače koji spajaju mreže različitih mrežnih podmaski. U LAN okruženju s uključenim IP dijeljenjem, mrežna vrata su zapravo usmjerivač. U uredu, mrežna vrata su uobičajeno multi-funlcionalni uređaji koji uključuju NAT, vatrozid, upravljanje s propusnosti i ostale sigurnosne funkcije.

Gubitak broz kablove i konektore
Za vrijeme kreiranja bežične mreže, potrebno je uključiti faktore gubitka kroz kablove i konektore. Gubitak kroz kablove i konektore smanjiti će izlaznu snagu kod pošiljatelja i jačinu signala kod primatelja. Što je veća duljina kabla to će biti veći gubici. Gubici kroz kabel trebaju se oduzeti od ukupne izlazne snage dok se računa udaljenost. Na primjer: ako je gubitak kroz kabel i konektore 3 dBm i izlazna snaga je 20 dBm tada je izlazna snaga kabla samo 17 dBm.

Hotspot
Mjesto gdje možete pristupiti Wi-Fi servisu. Izraz *Hotspot* ima dva značenja u bežičnom okruženju. Jedno je pružanje bežične infrastrukture, a drugo je sustav naplata pristupa Internetu. U Hotspot sustavu, pružatelj usluga treba: autetifikacijski sustav, sustav upravljanja računima i naplate te bežični AP mrežu za pružanje usluge korisnicima.

IGMP Snooping

Internet Group Management Protocol (IGMP) je protokol trećeg sloja koji služi za uspostavu *multicast* grupa. *IGMP snooping* je opcija koja omogućuje Ethernet prespojniku „slušanje“ IGMP komunikacije između klijenta i usmjerivača. Prespojnici koji podržavaju IGMP *snooping* imaju mogućnost izbjegavanja *multicast* prometa koji se tretira kao *broadcast* promet i zbog toga smanjuju ukupan promet u mreži.

Infrastructure Mode (Infrastrukturni način)

Bežična mreža koja je napravljena oko jedne ili više pristupne točke sa svrhom pružanja pristupa bežičnim klijentima žičanim LAN / internet servisima.

IP adresa

IP (Internet Protocol) je protokol trećeg sloja koji predstavlja osnovu sve internet komunikacije. IP adresa je 32-bitni broj koji identificira klijenta koji šalje ili prima poruke putem interneta. IP adresa sastoji se od dva dijela: prvi dio predstavlja identifikaciju određene mreže na internet, a drugi dio odnosi se na određeni uređaj (koji može biti poslužitelj ili radna stanica) unutar mreže. IPv6 specifikacija podržava 128-bitni IP format.

IPsec

IP Security. Skup protokola koje su razvili IETF za podržavanje sigurne izmjene paketa kroz IP sloj. IPsec razvijen je s ciljem implementiranja u VPN (Virtual Private Networks) mreže. IPsec podržava dvije enkripcijske metode: *Transport* i *Tunnel*. Transportna enkripcija šifrira samo podatke svakog paketa, ali ne i zaglavlje dok tuneliranje šifrira podatke i zaglavlje. Strana koja prima IPsec pakete dešifrira svaki paket.

Klijent

Klijent je mrežni uređaj koji prima servis od poslužitelja. Izraz klijentski uređaj podrazumijeva krajnji korisnički uređaj poput bežične mrežne kartice ili bežični CPE.

Kontrola prijenosa (Rate Control)

Ethernet ima funkciju za kontrolu brzine postavljanja i preuzimanja svakog individualnog porta. Upravljanje kontrolom brzine prijenosa koristi *Flow Control* za ograničavanje brzine porta. Zbog toga, Ethernet adapter također mora imati omogućenu *Flow Control* opciju. Jedan on načina za prisiljavanje *Flow Control* adaptera je postavljanje porta na polu-dupleks.

Kontrola prometa (Bandwidth Management)
Upravljanjem propusnosti kontroliramo brzinu prijenosa porta, korisnika, IP adrese i aplikacije. Usmjerivač može koristiti kontrolu propusnosti za limitiranje brzine internet veze određene IP adrese ili aplikacije. Također može garantirati definiranu brzinu određene aplikacije ili privilegirane IP adrese što predstavlja osnovnu funkciju QoS-a (Quality of Service).

LACP (802.3ad) Trunking
802.3ad *Link Aggregation* standard definira kako kombinirati nekoliko Ethernet portova u jedan veliki propusni port za povećanje prijenosne snage. Također je poznat pod nazivom *Port Trunking*. Za ispravan rad, obje strane koje sudjeluju u komunikaciji moraju omogućiti opciju.

MAC
Media Access Control. MAC adresa je identifikator drugog sloja za mrežne uređaje. Svaki Ethernet uređaj ima jedinstvenu adresu. Prvih 6 znamenki predstavljaju jedinstvenu oznaku proizvođača. Kada je unutar mreže uključena MAC kontrola pristupa, samo uređaji s ovlaštenim MAC adresama mogu se spojiti na mrežu.

Maska podmreže
Adresni kod, koji određuje veličinu mreže. IP podmreže određuju se pomoću *BIT-wise AND operatora* između IP adrese i maske podmreže. Promjenom maske podmreže, možete promijeniti opseg i veličinu mreže.

Mb/s
Megabit po sekundi. Milion bita po sekundi, jedinica mjerenja za prijenos podataka.

MESH
MESH je vanjska bežična tehnologija koja koristi STP (Spanning Tree Protocol) protokol i WDS (Wireless Distribution System) sustav za postizanje samo-formirane i samo-konfigurirane vanjske mreže. MESH mreže imaju mogućnosti pronaći najkraći put do udaljenog odredišta.

MIMO
Multi In Multi Out. Tehnologija koja povećava pokrivenost i performanse WLAN mreže. Unutar MIMO uređaja dvije ili više antena koriste se za povećanje osjetljivosti primatelja i za povećanje fokusa dostupne snage prema namijenjenom Rx.

Nadogradnja
Zamjenjuje trenutni softver ili firmver s novom verzijom.

NAT
Network Address Translation. Mrežni algoritam kojeg koriste usmjerivači kod dijeljenja jedne IP adrese između više korisnika. IP adresa koju usmjerivač dobije od ISP-a zove se vanjska IP adresa, a IP adresa koja je dodijeljena od NAT protokola zove se privatna IP adresa.

Osjetljivost primatelja (Receiver Sensitivity)
Osjetljivost primatelja predstavlja osjetljivost primljenog radio signala. Općenito, što je prijenos sporiji, veća je osjetljivost. Osjetljivost primatelja mjeri se u dB; što je niža apsolutna vrijednost, to je jači signal. Na primjer, -50dB je više od -80dB.

Paket
Jedinica podataka koja se šalje kroz mrežu.

Passphrase
Slična zaporki.

Podmreža (Subnetwork ili Subnet)
Koristi se u velikim mrežama. Manje mreže koriste se za adresiranje između velikog broja računala. Podmreže su spojene na glavnu mrežu uz pomoć usmjerivača, koncentratora ili mrežnih vrata. Svaki individualni bežični LAN koristiti će istu podmrežu za komuniciranje s ostalim računalima u mreži.

POE
Power over Ethernet. Standard koji omogućuje isporuku napajanja i struje putem jednog Ethernet kabla (UTP/STP). Omogućuje instalaciju mrežnih uređaja daleko od izvora napajanja. PoE sustav se uobičajeno sastoji od dvije komponente: DC ubrizgivač (osnovna jedinica) i razdjelnik (terminalna jedinica). DC ubrizgivač kombinira struju i podatke, dok ih razdjelnik razdvaja. PoE pristupne točke ili CPE imaju ugrađeni razdjelnik unutar uređaja. IEEE 802.3af je PoE specifikacija koja koristi 48 volti za isporuku struje do 100 metara udaljenosti.

Port
Postoje dva različita značenja u mrežnom svijetu:

- Hardverska pristupna točka na računalu ili mrežnom uređaju koja se koriste za spajanje kabla ili adaptera.
- Virtualna pristupna točka kroz koju računalo koristi posebnu aplikaciju na poslužitelju.

Postavljanje (Upload)
Slanje datoteke na mrežni uređaj putem interneta.

PPPoE
Point-to- Point Protocol over Ethernet. PPPoE oslanja se na dva raširena standarda, a to su PPP i Ethernet. PPPoE predstavlja specifikaciju za spajanje korisnika na internet koji se nalaze u Ethernet okruženju kroz uobičajeno širokopojasni pristup poput DSL linije, bežičnog uređaja ili kablovskog modema.

PPTP
Point-to-Point Tunneling Protocol: VPN protokol koji je razvio PPTP forum. Putem PPTP korisnici mogu pristupiti korporativnim mrežama putem Interneta. Ukoliko korisnici zahtijevaju šifriranje podataka kada koriste Windows PPTP klijent, tada udaljeni VPN poslužitelj mora podržavati MPPE (Microsoft Point-To-Point Encryption Protocol) enkripciju. PPTP koriste i neki ISP za autentifikaciju korisnika.

Preambula
Preambule se šalju sa svakim bežičnim paketom radi statusa prijenosa. Duga preambula koristi se za bolju kompatibilnost, a kratka za bolje performanse.

Premosnik (Bridge)
Uređaj koji spaja dvije različite mreže koje koriste isti protokol. Bežični premosnici se uobičajeno koriste za povezivanje mreža udaljenih zgrada. Postoje dvije vrste premosnika. WDS premosnik može se koristiti kao *Point-to-Point* ili kao *Point-to-Multipoint* topologija. Premosna infrastruktura može se koristiti kao AP za formiranje mrežne topologije.

Pristupna točka (AP)
Centralni koncentrator bežične LAN mreže. Pristupne točke imaju jedan ili više Ethernet portova na koje se uređaju mogu spojiti (poput internet veze). Multi-funkcionalne pristupne točke mogu raditi kao Ethernet klijent, bežični premosnik ili mogu pojačavati signale drugih pristupnih točaka. Pristupne točke uobičajeno imaju više bežičnih funkcije nego bežični usmjerivači.

RADIUS
Remote Authentication Dial-In User Service. Autentifikacijski i upravljački sustav kojeg koriste brojni pružatelji internet usluga (ISP). Kada se spajate na ISP morate upisati svoje korisničko ime i zaporku. Podaci se prosljeđuju prema RADIUS poslužitelju, koji provjerava ispravnost informacija i tada omogućuje pristup prema ISP sustavu. RADIUS tipično koristi 1812 i 1813 portove za autentifikaciju i upravljanje. Iako nije službeni standard, RADIUS specifikacije održava radna grupa IETF.

RJ-45
Standardni konektori za uparene parice koji se koriste u Ethernet mrežama. Iako izgledaju slično RJ-11 telefonskim konektorima, RJ-45 mogu imati do osam žica, dok telefonski konektori imaju samo četiri.

RTS
Request To Send. Paket koji se šalje kada računalo želi prenijeti podatke. Računalo će čekati na CTS (Clear to Send) poruku prije nego počne slati podatke.

RTS Threshold
RTS/CTS (Request to Send/Clear to Send) paket će biti poslan prije okvira, ako je okvir veći od zadane vrijednosti. Smanjenje vrijednosti može poboljšati performanse u slučaju velikog broja korisnika u mreži. Kada imate veliki broj klijenata u mreži, možete probati postaviti vrijednost na 1500, 1000 ili 500.

Snaga signala
Snaga signala je vrijednost koja pokazuje osjetljivost primanja udaljenog bežičnog uređaja. Općenito, udaljene pristupne točke s jačim signalom prikazivati će veću vrijednost. Što je manja apsolutna vrijednost, to je signal jači. Na primjer: -50dB ima jači signal nego -80dB. Za vanjsku upotrebu, signal koji je jači od -60dB smatra se dobrom vezom.

SNMP
Simple Network Management Protocol. Skup protokola koji služe za upravljanje složenim mrežama. SNMP mreža sadrži tri ključna elementa: upravljive uređaje, agente i NMS (Network Management Systems). Upravljivi uređaji su mrežni uređaji koji sadrže SNMP agente. SNMP agenti su programi koji se nalaze unutar firmvera SNMP uređaja za pružanje usluge SNMP konfiguracije. NMS uobičajeno predstavlja računalni softver poput HP OpenView-a koji može vidjeti i upravljati udaljenim SNMP mrežnim uređajima.

SSH

Razvio ga je SSH Communications Security Ltd. Secure Shell je program za prijavu na drugo računalo putem mreže, za izvršavanje naredbi na udaljenoj mašini i za premještanje dokumenata s jedne mašine na drugu. Pruža jaki autentifikacijski sustav i sigurnu komunikaciju putem nesigurnih kanala. Predstavlja zamjenu za rlogin, rsh, rcp i rdist.

SSL

Secure Sockets Layer. Popularni enkripcijski sustav kojeg koriste brojne online trgovine i bakarski portali za zaštitu financijskih transakcija. Kada započne SSL sesija, poslužitelj pošalje javni ključ pretraživaču. Pretraživač nakon toga šalje poslužitelju nasumično izabrani tajni ključ u svrhu razmjene tajnog ključa za tu sesiju. SSL VPN također je poznat pod nazivom Web VPN. HTTPS i SSH upravljačko sučelje koriste SSK za šifriranje podataka.

TCP

Protokol četvrtog sloja koji se zajedno s IP protokolom koristi za slanje podataka između računala putem interneta. IP se brine za stvarnu isporuku podataka, dok se TCP brine da se paketi ispravno prenesu putem interneta.

Tx izlazna snaga

Predstavlja izlaznu snagu signala. U normalnim situacijama, Tx izlazna snaga za 2.4 GHz 11g/b je 20 dBm na kraju antene, dok je recimo za 5 GHz 802.11a 30 dBm.

UDP

User Datagram Protocol. Pripada četvrtom sloju i služi za prijenos podataka koji ne zahtijevaju potvrdu primitka od primatelja.

Usmjerivač

IP usmjerivač je uređaj koji omogućuje dijeljenje jedne IP adrese između više klijenata koristeći NAT tehnologiju. Bežični usmjerivač je uređaj koji kombinira funkcije pristupne točke i IP usmjerivača.

Vatrozid (Firewall)
Sustav koji osigurava mrežu i sprječava pristup neovlaštenim korisnicima. Vatrozid može biti softverski ili hardverski (usmjerivač, mrežna vrata). Vatrozid sprečava neovlašteni pristup mreži, a isto tako može ograničiti slanje podataka iz mreže.

URL
Uniform Resource Locator. Adresa dokumenta na internetu.

VPN
Virtual Private Network. Tehnologija koja služi za povećanje sigurnosti kod prijenosa podataka putem interneta. VPN stvara privatni šifrirani tunel od korisničke strane koja šalje/prima podatke, kroz lokalnu bežičnu mrežu, internet pa sve do korporativne mreže.

WAN
Wide Area Network. Komunikacijski sustav koji spaja računala ili druge uređaje kroz veliko, lokalno, regionalno, nacionalno ili internacionalno geografsko područje. WAN port na mreži predstavlja port (ili bežičnu vezu) koji je spojen s internet strane mrežne topologije.

WEP
Wired Equivalent Privacy. Bežični protokol za šifriranje. Dostupan je kao 40-bitni (64-bitni), 108-bitni (128-bitni) ili 152-bitni enkripcijski model.

Wi-Fi
Wireless Fidelity. Predstavlja interoperabilni certifikat za bežične loklane mreže (LAN) koji su bazirani na IEEE 802.11 standardu. Odgovorno tijelo za Wi-Fi je Wi-Fi Alliance, poznato pot nazivom WECA.

WiMAX
Predstavlja interoperabilnost za *Microwave Access*. WiMAX je WMN (Wireless Metropolitan Network*)* tehnologija koja se oslanja na IEEE 802.16 i ETSI *Hiperman* standarde. Originalni 802.16 standard imao je radnu frekvenciju od 10 do 66 GHz. 802.16a predstavlja nadopunu originalnog standarda i ima raspon od 2 do 11 GHz. 802.16d povećava brzinu prijenosa podataka između 40 do 70 Mb/s te podržava MIMO antene i QoS. 802.16e dodaje mobilne funkcionalnosti, uži pojas (do maksimalno 6 MHz), manju brzinu i manje antene.

WDS

Wireless Distribution System. WDS definira koliko bežičnih pristupnih točaka ili bežičnih usmjerivača se može zajedno spojiti u jednu bežičnu mrežu bez korištenja žičane veze.

WLAN

Wireless Local Area Network. Vrsta lokalne mreže koja koristi visoko frekvencijske valove umjesto žica za komuniciranje između čvorova. Najpopularniji WLAN standard je 802.11.

WMM

Wi-Fi Multimedia (WMM) je standard za multimedijske aplikacije. WMM prioritizira VoIP, zvučni, video i streaming promet, a također i tradicionalni IP promet kroz pristupne točke.

WMS

Wireless Management System. Program koji služi za upravljanje bežičnim pristupnim točaka / premosnicima.

WPA

Wi-Fi Protected Access. Napredni enkripcijski standard koji je predložio WiFi za pružanje napredne zaštite uz pomoć ključa (TKIP) ili certifikata. Daleko je sigurni nego WEP enkripcija. WPA-PSK koristi unaprijed dijeljeni ključ za enkripciji / autentifikaciju.

WPA2

Wi-Fi Protected Access 2. WPA2 je poznat pod nazivom 802.11i. WPA sigurnost povećava uz pomoć CCMP i AES enkripcije. WPA2 je kompatibilan s WPA. WPA2-PSK koristi unaprijed dijeljeni ključ za enkripciji / autentifikaciju.